



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N° 178

SEMANA DEL 25 DE NOVIEMBRE AL 1 DE
DICIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

1

Las mitigaciones son útiles en productos de Google.



IP INFORMADAS

17

Listado de IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

25

Asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

7

Asociadas a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

1. Malware	3
2. Sitios fraudulentos	4
3. Phishing	6
4. Fuerza Bruta	10
5. Vulnerabilidades	11
6. Concientización	12
7. Recomendaciones y buenas prácticas.....	13
8. Muro de la Fama.....	14



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

1. Malware



CSIRT alerta ante campaña de phishing con malware, que suplanta a Extral

Alerta de seguridad cibernética	2CMV22-00390-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de noviembre de 2022
Última revisión	29 de noviembre de 2022

Indicadores de compromiso

Asunto

Facturacion electronica

Correo de Salida

chernandez@extral.com.mx

SHA256

bc74667556dc9f935ea423d6027c494a1daf8db07225ad278afc0614cb1158d5
3d5d6044734a18b4a78abaa64326d544e3e6aaa8a68f1e86a1fce05c1c90ade6
8139c3fe860410dee6c76c9bc1ababc163043f9d4784ed468fe8a25a7c0eae41
4dc59c4e6f73f6c9c17a40fe2fe0a74670b6a0b712b73a002ec497848894dd5d
005e51bcc1decf20239bb92a0411f669c2ad26c86839754ee34a43a2d020afa7
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4

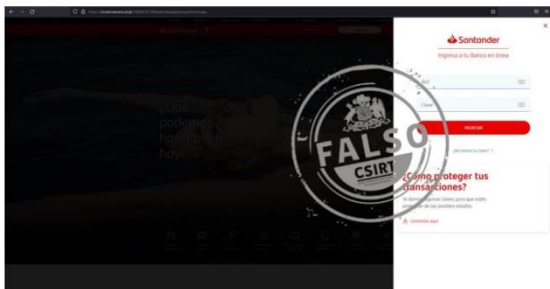
Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00390-01/>

<https://www.csirt.gob.cl/media/2022/11/2CMV22-00390-01.pdf>

2. Sitios fraudulentos

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta al Banco Santander

Alerta de seguridad cibernética	8FFR22-01148-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2022
Última revisión	25 de noviembre de 2022

Indicadores de compromiso

URL sitio falso

<http://bit.ly/3tCROKm>

https://tarjetas-estado.click/lveversion/url?source=uact&ref_=ojp2ebmmfclgab

Dirección IP

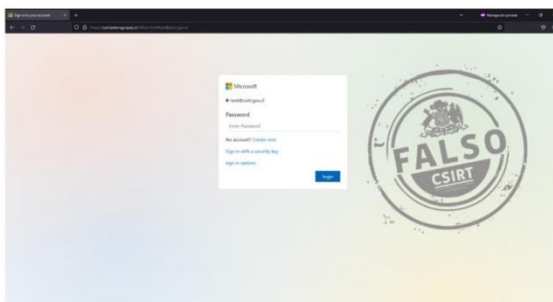
[104.21.9.63]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01148-01/>

<https://www.csirt.gob.cl/media/2022/11/8FFR22-01148-01.pdf>

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta login de email de Microsoft

Alerta de seguridad cibernética	8FFR22-01149-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2022
Última revisión	25 de noviembre de 2022

Indicadores de compromiso

URL sitio falso

<https://santaelenagrapes.cl/office.html#test@csirt.gob.cl>

Dirección IP

[200.73.115.38]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01149-01/>

<https://www.csirt.gob.cl/media/2022/11/8FFR22-01149-01.pdf>

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO





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

Imagen del sitio		CSIRT alerta ante nueva campaña de phishing con malware		
	Alerta de seguridad cibernética	8FFR22-01150-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	29 de noviembre de 2022		
	Última revisión	29 de noviembre de 2022		
	Indicadores de compromiso			
	URL sitio falso			
	https://sagat[.]cl/eed/prepaid/ https://sagat[.]cl/eed/prepaid/\$/ https://sagat[.]cl/eed/prepaid/\$/signin?cmd=Chile&code=CL			
Dirección IP				
[190.13.188.108]				
Enlaces para revisar el informe:				
https://www.csirt.gob.cl/alertas/8ffr22-01150-01/ https://www.csirt.gob.cl/media/2022/11/8FFR22-01150-01.pdf				

Imagen del sitio		CSIRT alerta de página fraudulenta que suplanta a LinkedIn		
	Alerta de seguridad cibernética	8FFR22-01151-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	29 de noviembre de 2022		
	Última revisión	29 de noviembre de 2022		
	Indicadores de compromiso			
	URL sitio falso			
	hXXps://carburo2.srtv[.]cl/wp-includes/blocks/linkedin.com/linkedin.com/login.php?dtfgt=%7B%7Bemail%7D%7D hXXps://carburo2.srtv[.]cl/wp-includes/theme-compat/linkedin.com/linkedin.com/login.php?email=test%40csirt.gov.cl			
Dirección IP				
[152.231.105.93]				
Enlaces para revisar el informe:				
https://www.csirt.gob.cl/alertas/8ffr22-01151-01/ https://www.csirt.gob.cl/media/2022/11/8FFR22-01151-01.pdf				

3. Phishing

Imagen del mensaje



CSIRT alerta ante campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00662-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de noviembre de 2022
Última revisión	25 de noviembre de 2022

Indicadores de compromiso

URL redirección
[https://nhmwcotitostado\[.\]info/activacion/cuenta-ulen/](https://nhmwcotitostado[.]info/activacion/cuenta-ulen/)

URL sitio falso
[https://yashevents\[.\]top/1669378947/imagenes/_personas/home/default.asp](https://yashevents[.]top/1669378947/imagenes/_personas/home/default.asp)

Dirección IP
[172.67.213.222]

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/alertas/8fph22-00662-01/>
<https://www.csirt.gob.cl/media/2022/11/8FPH22-00662-01.pdf>

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH22-00663-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2022
Última revisión	28 de noviembre de 2022

Indicadores de compromiso

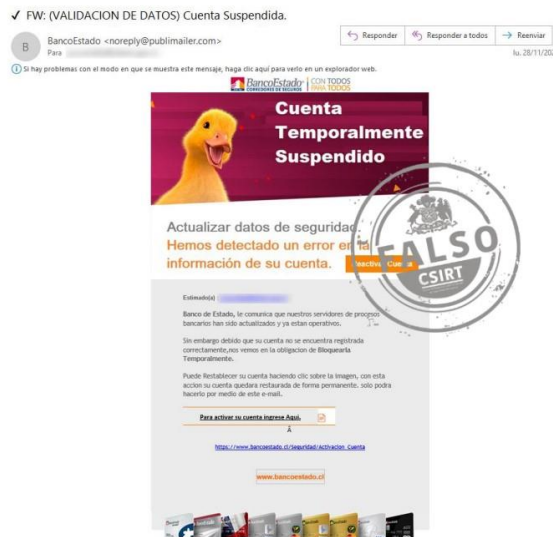
URL redirección
[https://bit\[.\]ly/3Ub4EKA?l=www.bancoripley.cl](https://bit[.]ly/3Ub4EKA?l=www.bancoripley.cl)
[https://prisonjailexpert\[.\]com/bancoripley/cuenta-sclv/](https://prisonjailexpert[.]com/bancoripley/cuenta-sclv/)

URL sitio falso
[https://web.bancoripley.cl.buckreality\[.\]net/1669637408/login](https://web.bancoripley.cl.buckreality[.]net/1669637408/login)

Dirección IP
[64.91.247.208]

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/alertas/8fph22-00663-01/>
<https://www.csirt.gob.cl/media/2022/11/8FPH22-00663-01.pdf>

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH22-00664-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2022
Última revisión	28 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://nhmwcotitostado\[.\]info/activacion/cuenta-ulen/](https://nhmwcotitostado[.]info/activacion/cuenta-ulen/)

URL sitio falso

[https://melekcopeur\[.\]club/1669657753/imagenes/_personas/home/default.asp](https://melekcopeur[.]club/1669657753/imagenes/_personas/home/default.asp)

Dirección IP

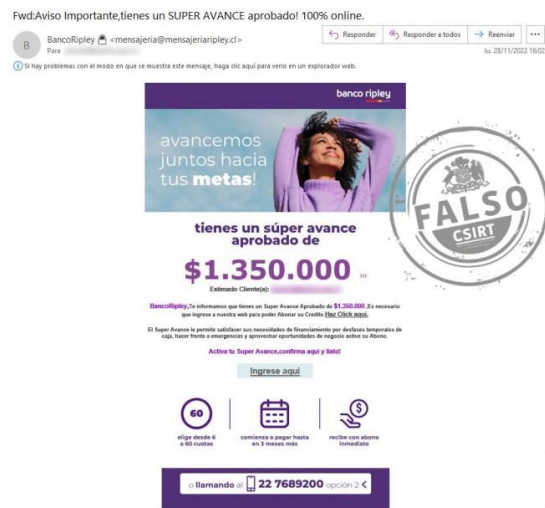
[172.67.145.74]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00664-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00664-01.pdf>

Imagen del mensaje



CSIRT alerta de campaña que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FPH22-00665-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2022
Última revisión	28 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://bit\[.\]ly/3FbKOLb?l=www.bancoripley.cl](https://bit[.]ly/3FbKOLb?l=www.bancoripley.cl)

[https://wordpress-413449-1536776.cloudwaysapps\[.\]com/bancoripley/cuenta-
iqdg/](https://wordpress-413449-1536776.cloudwaysapps[.]com/bancoripley/cuenta-iqdg/)

URL sitio falso

[https://web.bancoripley.cl.buckreality\[.\]net/1669662421/login](https://web.bancoripley.cl.buckreality[.]net/1669662421/login)

Dirección IP

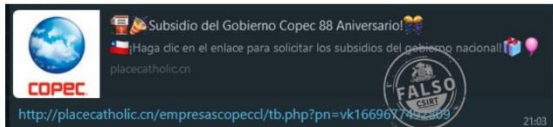
[64.91.247.208]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00665-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00665-01.pdf>

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta a Copec

Alerta de seguridad cibernética	8FPH22-00666-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2022
Última revisión	28 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://8yue22\[.\]cn/J4gzk8b6/empresascopecl/?_t=1669680590470#1669680592761](https://8yue22[.]cn/J4gzk8b6/empresascopecl/?_t=1669680590470#1669680592761)

URL sitio falso

[https://8yue22\[.\]cn/J4gzk8b6/empresascopecl/?_t=1669680590470#1669680592761](https://8yue22[.]cn/J4gzk8b6/empresascopecl/?_t=1669680590470#1669680592761)

Dirección IP

[104.21.77.105]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00666-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00666-01.pdf>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00667-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022

Indicadores de compromiso

URL redirección

[https://nhmwcotitostado\[.\]info/activacion/cuenta-ulen/](https://nhmwcotitostado[.]info/activacion/cuenta-ulen/)

URL sitio falso

[https://chezcrom\[.\]com/1669734595/imagenes/_personas/home/default.asp](https://chezcrom[.]com/1669734595/imagenes/_personas/home/default.asp)

Dirección IP

[104.21.88.186]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00667-01/>

<https://www.csirt.gob.cl/media/2022/11/8FPH22-00667-01.pdf>

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

<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

Fwd:Aviso black-friday, tienes un SUPER AVANCE aprobado! 100% pídelo online.
BancoRipley <mensaje@mensaje@ripley.cl>
Para: bomear@interior.gob.cl mi: 30/11/2022 2:18



CSIRT alerta de campaña de phishing que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FPH22-00668-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de noviembre de 2022
Última revisión	30 de noviembre de 2022

Indicadores de compromiso

URL redirección

<https://bit.ly/3VE72e1?l=www.bancoripley.cl>
<https://www.miteg.com.co/bancoripley/cuenta-buld/>

URL sitio falso

<https://web.bancoripley.cl.buckreality.net/1669814271/login>

Dirección IP

[64.91.247.208]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00668-01/>
<https://www.csirt.gob.cl/media/2022/11/8FPH22-00668-01.pdf>

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

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

4. Fuerza Bruta

 <p>ALERTA DE Fuerza Bruta</p> <p>4IIA21-00056-01 CSIRT alerta de ataques de fuerza bruta contra SMTP</p> <p>PARA REGISTRAR 562 2486 3850 UN INCIDENTE www.csirt.gob.cl</p> 	CSIRT alerta de ataques de fuerza bruta contra el protocolo SMTP	
	Alerta de seguridad cibernética	4IIA22-00056-01
	Clase de alerta	Intentos de Intrusión
	Tipo de incidente	Intentos de acceso – Fuerza bruta
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	28 de noviembre de 2022
	Última revisión	28 de noviembre de 2022
	Indicadores de compromiso	
	Direcciones IP	
103.14.225.215		
45.139.105.111		
37.139.128.9		
37.139.128.22		
185.246.221.244		
187.9.120.131		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/alertas/4iia22-00056-01/		
https://www.csirt.gob.cl/media/2022/11/4IIA22-00056-01.pdf		

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

5. Vulnerabilidades



CSIRT informa parche para nueva vulnerabilidad de Google Chrome

Alerta de seguridad cibernética	9VSA22-00749-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2022
Última revisión	28 de noviembre de 2022

CVE

CVE-2022-4135

Fabricantes

Bitbucket y Crowd

Productos afectados

Chrome anteriores a 107.0.5304.121 para macOS y Linux y a 107.0.5304.121/.122 para Windows.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00749-01/>

<https://www.csirt.gob.cl/media/2022/11/9VSA22-00749-01.pdf>

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

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

6. Concientización

Ciberconsejos para una pyme más segura

La seguridad digital es hoy en día tan importante como la física para cualquier empresa, no importando su tamaño. Por eso es que compartimos en esta ocasión seis ciberconsejos que pueden ayudar a las pymes a operar con mayor ciberseguridad.



Seis #ciberconsejos para una pyme más segura

1. Capacitar sobre los riesgos cibernéticos

Las personas **somos el eslabón más débil** en ciberseguridad. Por eso, es clave que estemos al día con los riesgos de internet y **realicemos capacitaciones periódicas** en temas como identificación de phishing, detección de fraudes y creación de contraseñas robustas a **todos los trabajadores** de tu empresa, sin importar su rango.



Seis #ciberconsejos para una pyme más segura

2. Establecer reglas de acceso

Tanto para los servidores y equipos de trabajo como para la red wifi de la empresa, debemos **definir reglas de acceso** seguras en términos **físicos y digitales**, además de contraseñas únicas.

Es importante que los empleados tengan acceso **solo a los sistemas que realmente necesitan utilizar**.



Seis #ciberconsejos para una pyme más segura

3. Respaldar la información

Es indispensable que realicemos **periódicamente copias de seguridad** de los datos y dispositivos computacionales que contengan información relevante para el negocio.


Estos respaldos **no deben** ser mantenidos en el mismo lugar físico que los originales. Además, debemos diseñar **planes de implementación** de los respaldos en el caso de perder los originales.



Seis #ciberconsejos para una pyme más segura





4. Mantener actualizado el software

Los ciberdelincuentes aprovechan cada vulnerabilidad que puedan encontrar en nuestras aplicaciones, por lo que resulta indispensable que cada vez que los fabricantes de software lancen **parches o actualizaciones** para resolver una vulnerabilidad, **la implementemos cuanto antes**, con el objetivo de proteger nuestra información.



Ver más: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-pymes-2022/>

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

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

7. 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 los sitios web que se ingresen sean los oficiales.

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

8. 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.

- 🛡️ Mauricio Alarcón
- 🛡️ Javier Lara
- 🛡️ Reynaldo Araya
- 🛡️ Natalia Crisóstomo
- 🛡️ Roberto Duarte

CONTACTO Y REDES SOCIALES DE CSIRT DE GOBIERNO

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