



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 191

SEMANA DEL 24 AL 2 DE MARZO 2023

INFORMACION IMPORTANTE

El CSIRT de Gobierno informa que debido a problemas técnicos, no ha sido posible publicar las alertas de seguridad cibernéticas y campañas de concientización en nuestro sitio web.

Por lo tanto, los informes e indicadores de compromiso los podrán encontrar en el repositorio de GitHub del CSIRT de Gobierno:
www.github.com/csirtcl

LA SEMANA EN CIFRAS

IP INFORMADAS

19

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



URL ADVERTIDAS

29

Asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

11

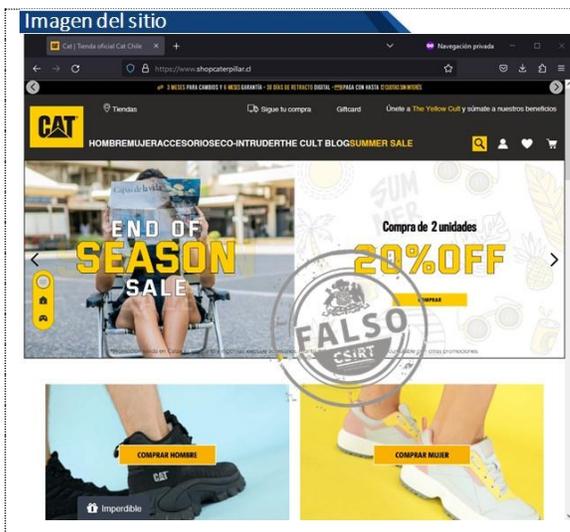
Asociadas a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

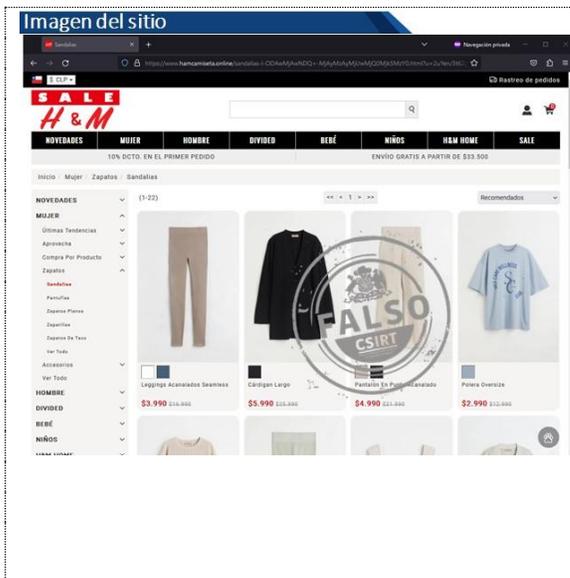
1.	Sitios fraudulentos	4
2.	Phishing	10
3.	Malware.....	14
4.	Concientización.....	15
5.	Recomendaciones y buenas prácticas	16
6.	Muro de la Fama	17

1. Sitios fraudulentos



CSIRT alerta sitio falso que suplanta a Caterpillar

Alerta de seguridad cibernética	8FFR23-01227-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de febrero de 2023
Última revisión	23 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.shopcaterpillar.[.]cl/	
Dirección IP	
[13.226.22.66]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01227-01.txt	



CSIRT advierte sitio que suplanta a H&M

Alerta de seguridad cibernética	8FFR23-01228-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2023
Última revisión	24 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://abrigoshop.flazio.[.]com/?gclid=Cj0KCCQjA3eGfBhCeARIsACpJNU-SsqpV1c5TqIIXGalFImGMf49x-D6-WwbpVcdNzPHZQBw_pCCnNYaAmPOEALw_wcB	
https://www.hamcamiseta.[.]online/?u=2uYen/3t6Zg=	
Dirección IP	
[162.218.176.46]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01228-01.txt	

Boletín de Seguridad Cibernética N° 191

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

BOLETÍN 13BCS23-00200-01 | SEMANA DEL 24 DE FEBRERO al 2 de MARZO DE 2023

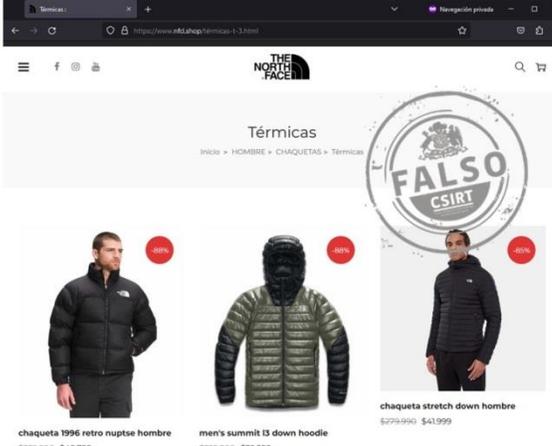
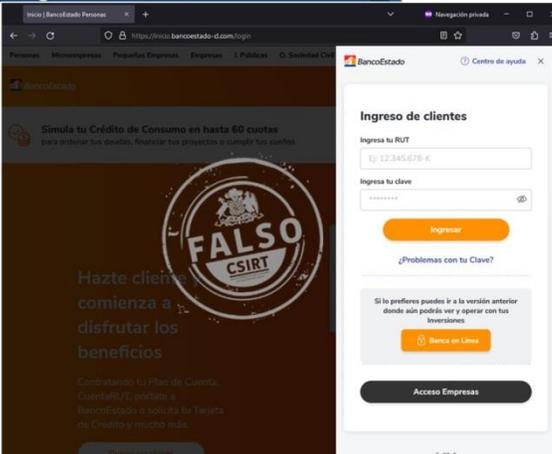
Imagen del sitio		CSIRT advierte sitio web que suplanta a The North Face		
	Alerta de seguridad cibernética	8FFR23-01229-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	27 de febrero de 2023		
	Última revisión	27 de febrero de 2023		
	Indicadores de compromiso			
	URL sitio falso	http[:]//www.nfcl[.]shop/		
	Dirección IP	[172.67.132.98]		
Enlace para revisar loC:				
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01229-01.txt				

Imagen del sitio		CSIRT alerta página web que suplanta a BancoEstado		
	Alerta de seguridad cibernética	8FFR23-01230-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	27 de febrero de 2023		
	Última revisión	27 de febrero de 2023		
	Indicadores de compromiso			
	URL sitio falso	https://is[.]jgd/ojfa8m		
	Dirección IP	[172.67.171.139]		
Enlace para revisar loC:				
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01230-01.txt				

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

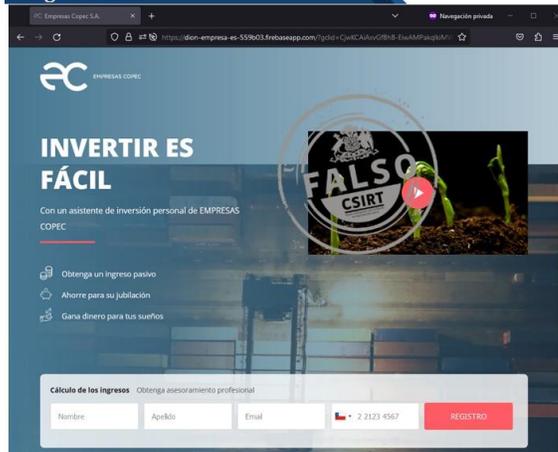
 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 191

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

BOLETÍN 13BCS23-00200-01 | SEMANA DEL 24 DE FEBRERO al 2 de MARZO DE 2023

Imagen del sitio



CSIRT advierte sitio que suplanta a Empresas Copec

Alerta de seguridad cibernética	8FFR23-01231-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023

Indicadores de compromiso

URL sitio falso

https://dion-empresa-es-559b03.firebaseio.com/?gclid=CjwKCAiAxxvGfBhB-EiwAMPakqliMwSelQ7bJ2qxSoom_J_U9a7yIRx9HN_LOopWgM8lQmsmRoei8BoC4O8QAvD_BwE

Dirección IP

[199.36.158.100]

Enlace para revisar IoC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01231-01.txt

Imagen del sitio



CSIRT alerta de página web que suplanta a Publimetro

Alerta de seguridad cibernética	8FFR23-01232-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023

Indicadores de compromiso

URL sitio falso

[https://zarinazira\[.\]com/?subid2=649023540604&subid3=www.csirt.gob.cl&gclid=EAlaIqobChMx57109q4_QIVUt9BR14vwL_EAEYASAAEgK7IPD_BwE](https://zarinazira[.]com/?subid2=649023540604&subid3=www.csirt.gob.cl&gclid=EAlaIqobChMx57109q4_QIVUt9BR14vwL_EAEYASAAEgK7IPD_BwE)

Dirección IP

[104.21.4.23]

Enlace para revisar IoC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01232-01.txt

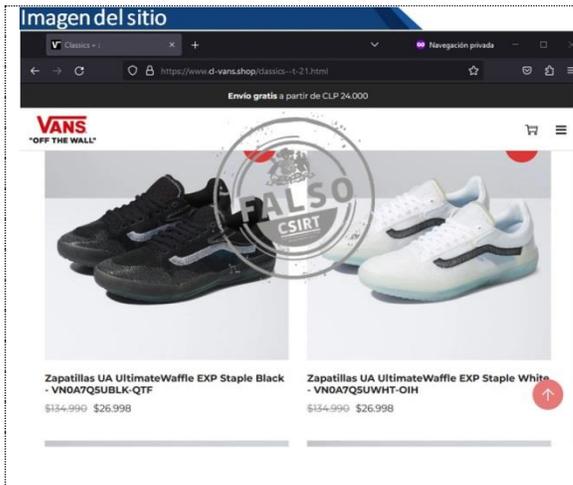
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 191

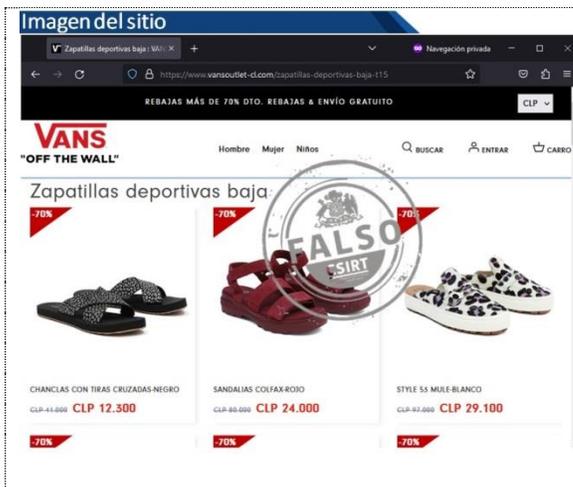
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00200-01 | SEMANA DEL 24 DE FEBRERO al 2 de MARZO DE 2023



CSIRT alerta sitio web falso de Vans

Alerta de seguridad cibernética	8FFR23-01233-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023
Indicadores de compromiso	
URL sitio falso https://www.cl-vans[.]shop/	
Dirección IP [104.21.6.155]	
Enlace para revisar IoC: https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01233-01.txt	



CSIRT advierte página web que suplanta a Vans

Alerta de seguridad cibernética	8FFR23-01234-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2023
Última revisión	2 de marzo de 2023
Indicadores de compromiso	
URL sitio falso https://www.vansoutlet-cl[.]com/	
Dirección IP [172.67.219.225]	
Enlace para revisar IoC: https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01234-01.txt	

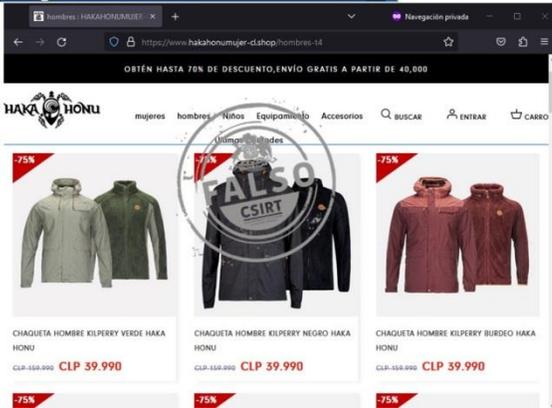
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

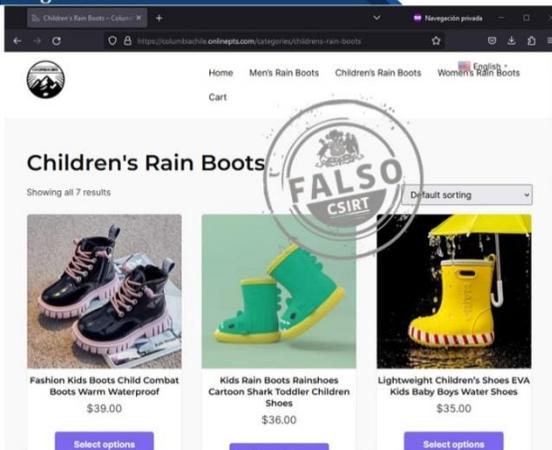
<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 191

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

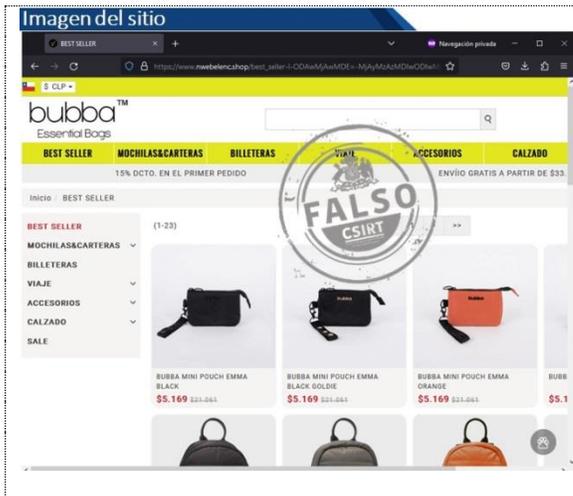
BOLETÍN 13BCS23-00200-01 | SEMANA DEL 24 DE FEBRERO al 2 de MARZO DE 2023

	CSIRT alerta de sitio web falso de Haka-Honu	
	Alerta de seguridad cibernética	8FFR23-01235-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	2 de marzo de 2023
	Última revisión	2 de marzo de 2023
	Indicadores de compromiso	
	URL sitio falso https://www.hakahonumujer-cl[.]shop/	

	CSIRT informa de página web que suplanta a Columbia	
	Alerta de seguridad cibernética	8FFR23-01236-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	2 de marzo de 2023
	Última revisión	2 de marzo de 2023
	Indicadores de compromiso	
	URL sitio falso https://columbiachile.onlinepts[.]com	

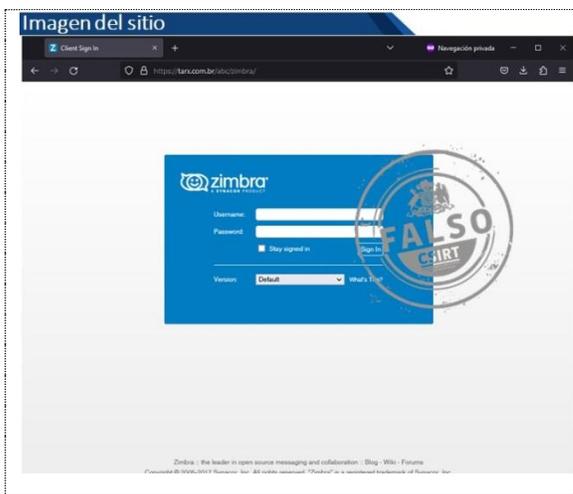
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



CSIRT advierte sitio web falso Bubba Bag

Alerta de seguridad cibernética	8FFR23-01237-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2023
Última revisión	2 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.nwebelenc[.]shop	
Dirección IP	
[23.252.71.142]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01237-01.txt	



CSIRT alerta página web falsa que suplanta a Zimbra

Alerta de seguridad cibernética	8FFR23-01238-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2023
Última revisión	2 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://tarx[.]com.br/abc/zimbra/	
Dirección IP	
[189.45.192.187]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01238-01.txt	

2. Phishing

Imagen del mensaje

Chilexpress: Usted tiene (1) encomienda retenida en nuestra BODEGA-SCL, para resolver este problema ingrese aquí: <https://amdel.cl>



11:11

CSIRT alerta de campaña de smishing que suplanta a Chilexpress

Alerta de seguridad cibernética	8FPH23-00757-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2023
Última revisión	24 de febrero de 2023

Indicadores de compromiso

URL redirección

<https://amdel.cl/>
[https://r.chilexpress\[.\]live/r/KlsMhSg](https://r.chilexpress[.]live/r/KlsMhSg)

URL sitio falso

[https://envios.chilexpress\[.\]live/Contingencia/f5e2d6abceb10c49b26c019d3f9fa30f](https://envios.chilexpress[.]live/Contingencia/f5e2d6abceb10c49b26c019d3f9fa30f)

Dirección IP

[94.242.53.110]

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00757-01.txt

Imagen del mensaje

Scotia: Se ha detectado un acceso no autorizado a tu cuenta. Por favor confirma tus datos aquí: <https://fastchile.cl>



CSIRT alerta campaña de smishing que suplanta al BancoScotia

Alerta de seguridad cibernética	8FPH23-00758-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2023
Última revisión	24 de febrero de 2023

Indicadores de compromiso

URL redirección

<https://fastchile.cl>
[https://r.sco-ingreso\[.\]live/r/Hjsh43s](https://r.sco-ingreso[.]live/r/Hjsh43s)

URL sitio falso

[https://personas.sco-ingreso\[.\]live/personas/Verificacion/b07c321213d96b0dd31bcbe59d75788c](https://personas.sco-ingreso[.]live/personas/Verificacion/b07c321213d96b0dd31bcbe59d75788c)

Dirección IP

[94.131.8.181]

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00758-01.txt

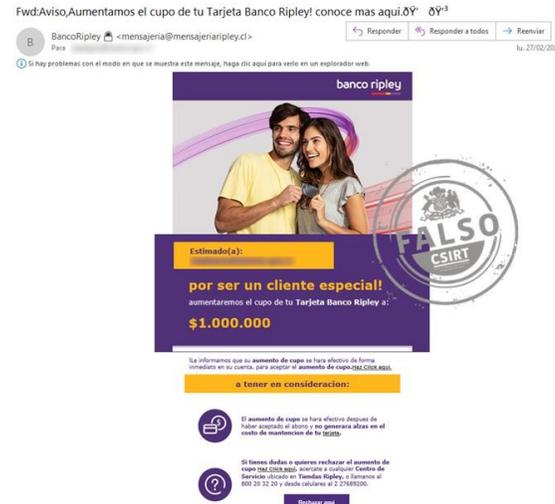
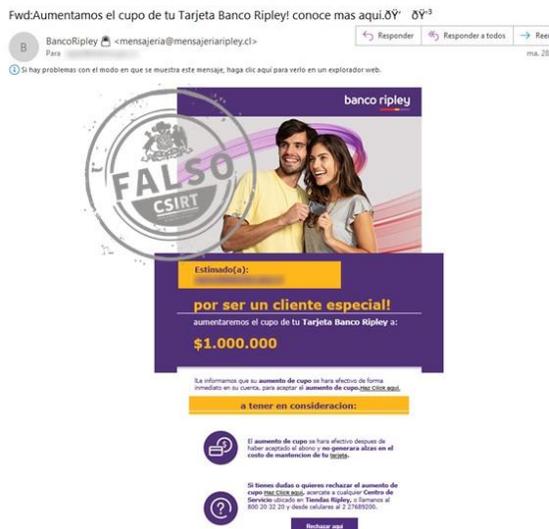
Imagen del mensaje		CSIRT advierte campaña de phishing que suplanta al Banco Ripley			
		Alerta de seguridad cibernética	8FPH23-00759-01		
		Clase de alerta	Fraude		
		Tipo de incidente	Phishing		
		Nivel de riesgo	Alto		
		TLP	Blanco		
		Fecha de lanzamiento original	27 de febrero de 2023		
		Última revisión	27 de febrero de 2023		
		Indicadores de compromiso			
		URL redirección		https://bit.ly/3Sup1mV?l=www.bancoripley.cl https://sam-tech.jp/bancoripley/cuenta-bshw/	
		URL sitio falso		https://web.banco-ripleycl.awadgallery.co.uk/1677500526/login	
Dirección IP		[148.113.159.144]			
Enlace para revisar loC:		https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00759-01.txt			

Imagen del mensaje		CSIRT informa campaña de phishing que suplanta al BancoEstado			
		Alerta de seguridad cibernética	8FPH23-00760-01		
		Clase de alerta	Fraude		
		Tipo de incidente	Phishing		
		Nivel de riesgo	Alto		
		TLP	Blanco		
		Fecha de lanzamiento original	28 de febrero de 2023		
		Última revisión	28 de febrero de 2023		
		Indicadores de compromiso			
		URL redirección		https://contawebnw.com/activacion/cuenta-wwnq/	
		URL sitio falso		https://nwmeponpatito.top/1677586479/imagenes/_personas/home/default.asp	
Dirección IP		[172.67.173.125]			
Enlace para revisar loC:		https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00760-01.txt			

Imagen del mensaje



CSIRT alerta campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH23-00761-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023

Indicadores de compromiso

URL redirección

[https://bit\[.\]ly/3Yb3X7?l=www.bancoripley.cl](https://bit[.]ly/3Yb3X7?l=www.bancoripley.cl)

[https://sam-tech\[.\]jip/bancoripley/cuenta-fvq/](https://sam-tech[.]jip/bancoripley/cuenta-fvq/)

URL sitio falso

[https://web.banco-ripleycl.awadgallery.co\[.\]uk/1677608708/login](https://web.banco-ripleycl.awadgallery.co[.]uk/1677608708/login)

Dirección IP

[148.113.159.144]

Enlace para revisar IoC:

https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00761-01.txt

Imagen del mensaje



CSIRT advierte campaña de phishing que suplanta a un inicio de sesión de correo electrónico.

Alerta de seguridad cibernética	8FPH23-00762-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023

Indicadores de compromiso

URL redirección

[https://webcentriscemsen.wapka\[.\]xyz/](https://webcentriscemsen.wapka[.]xyz/)

URL sitio falso

[https://webcentriscemsen.wapka\[.\]xyz/](https://webcentriscemsen.wapka[.]xyz/)

Dirección IP

[173.212.225.42]

Enlace para revisar IoC:

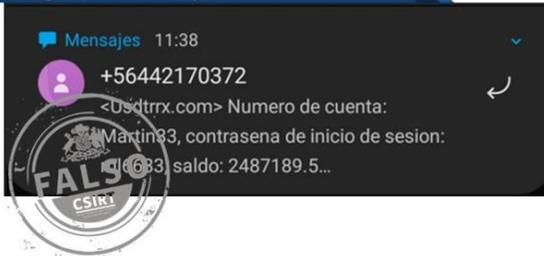
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00762-01.txt

Boletín de Seguridad Cibernética N° 191

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

BOLETÍN 13BCS23-00200-01 | SEMANA DEL 24 DE FEBRERO al 2 de MARZO DE 2023

Imagen del mensaje



CSIRT advierte campaña de smishing que suplanta un inicio de sesión de billetera de criptomonedas

Alerta de seguridad cibernética	8FPH23-00763-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero de 2023

Indicadores de compromiso

URL redirección

Usdtrrx[.]com

URL sitio falso

Usdtrrx[.]com

Dirección IP

[92.242.187.58]

Enlace para revisar IoC:

https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00763-01.txt

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

3. Malware

Imagen del mensaje



CSIRT advierte campaña de phishing con malware que suplanta a la Fiscalía General de la República

Alerta de seguridad cibernética	2CMV23-00401-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2023
Última revisión	24 de febrero de 2023

Indicadores de compromiso

Asunto

Mensaje importante! ID: (205969)

Correo de Salida

root@vghj27.adslmails.com

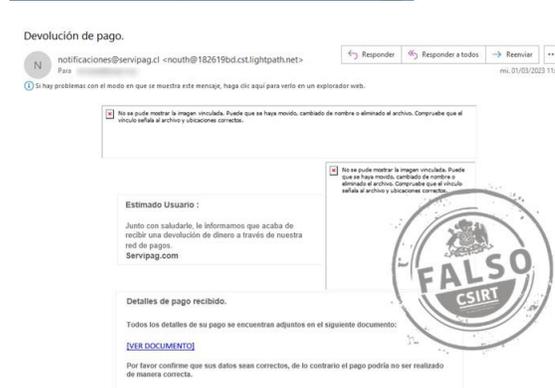
SHA256

8c2e2fede8c77f25b1555daf88461e0346c76218cba0ed6ada937c303e5cd8e868f74d929f9a07e87fa3927a1f762d9ce8611532345c2bc4c6e443dbfcbce24e8be9f858306daf9c886f5e579db2f788a21a5531c7d0028b6d663fac43ffaeb0c447670a3d9e3843a7d1758eb77842c8b5a9cd817ee1bc335c5adce43df64fa8b

Enlace para revisar IoC:

https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00401-01.txt

Imagen del mensaje



CSIRT advierte campaña de phishing con malware que suplanta a Servipag

Alerta de seguridad cibernética	2CMV23-00402-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2023
Última revisión	2 de marzo de 2023

Indicadores de compromiso

Asunto

Devolución de pago.

Correo de Salida

nouth@182619bd.cst.lightpath.net

SHA256

01fcca3d6d70126fe0f6bcbcb6ebd118571daca4a6651f5cb4c8fe478ca70d895b5ef9f0acea3657ccc51a932cedd2af09c12126aa5af39d6f0e83813491d6691440f247ae6bc6ad94848099db55962ea4068287776e8301e97c6a3990b7a1be4447670a3d9e3843a7d1758eb77842c8b5a9cd817ee1bc335c5adce43df64fa8bca9aa6aedb8d8b60138a8fc23a39a82dd0aac7d93bd43d7aaaf726e69c359d2943b8fa243f0fc5c5c175b7c0dd80390446c74f284107e4a16b8198f60183b0cb98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b

Enlace para revisar IoC:

https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00402-01.txt

4. Concientización

Ciberconsejos para no caer en falsas ofertas laborales

Si estás buscando trabajo, ten cuidado con las falsas ofertas laborales, ya que algunos de ellos buscan robar dinero o los datos de tus tarjetas bancarias. Esta semana en nuestros ciberconsejos te entregamos algunas recomendaciones para evitar caer en una estafa.



CIBERCONSEJOS
para no caer en falsas
ofertas laborales

RECOMENDACIONES

- **DESCONFÍA** de ofertas laborales con faltas de ortografía o mal redactados.
- **ASEGÚRATE** que la información sea coherente.
- **BUSCA** en un buscador información histórica de la empresa.
- **NUNCA** realices una transacción o pago durante el proceso de postulación ni entregues información bancaria.
- **SOSPECHA** de los anuncios que ofrecen buena remuneración sin solicitar experiencia previa.
- **DUDA** si utilizan cuentas de correo como Gmail o Hotmail.



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

5. 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 DEL CSIRT DE GOBIERNO

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

6. 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.

- David Mondaca
- Miguel Sandoval
- Nicole Jiménez
- Jean Pierre Olea
- Walter Cortés
- Felipe Cortés

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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