CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 192

SEMANA DEL 3 AL 9 DE MARZO 2023

INFORMACIÓN 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

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

URL ADVERTIDAS

19 asociadas a sitios fraudulentos y campañas de phishing y malware

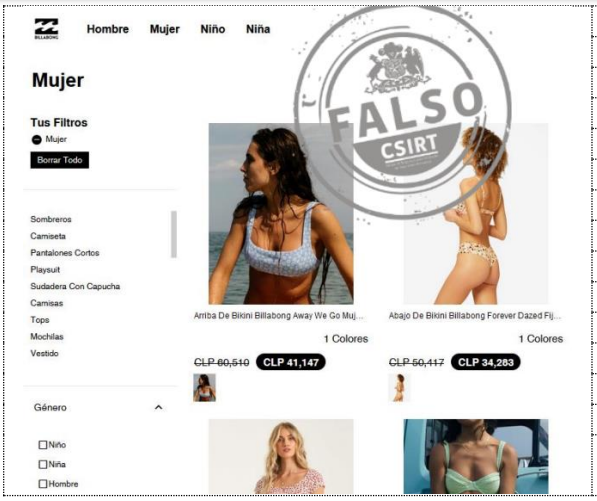
HASH REPORTADOS

7 asociadas a múltiples campañas de phishing con archivos que contienen malware

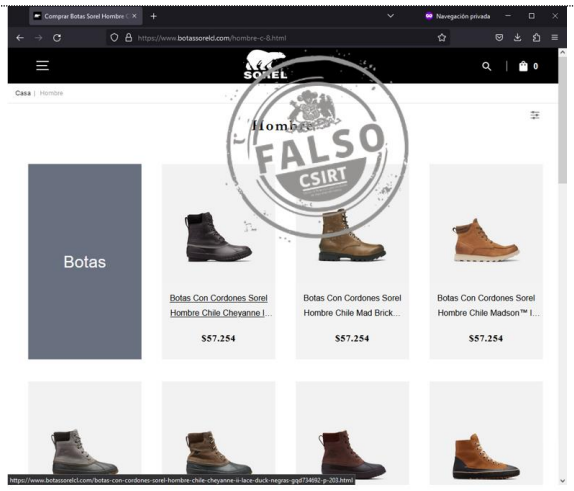
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

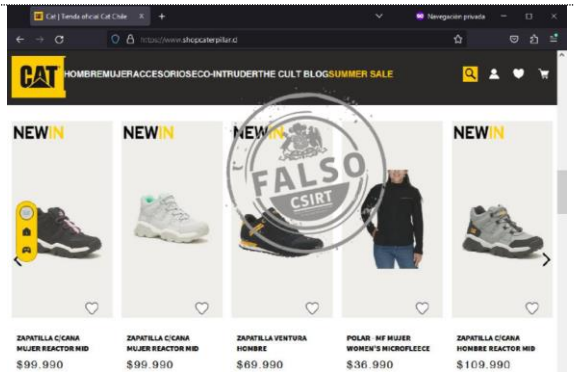
1. Sitios fraudulentos



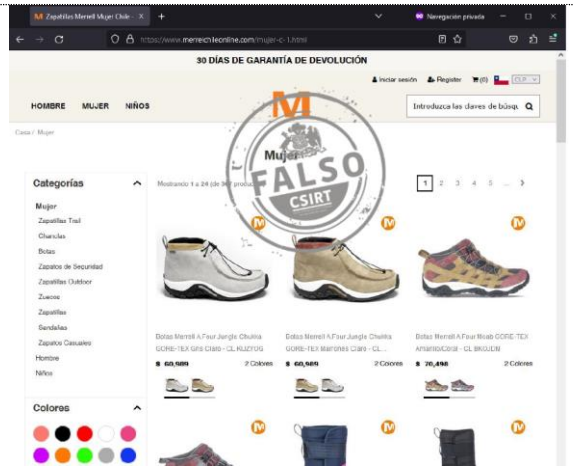
CSIRT advierte sitio que suplanta a Billabong	
Alerta de seguridad cibernética	8FFR23-01239-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.billabongchile[.]com/	
Dirección IP	
[196.247.61.208]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01239-01.txt	



CSIRT alerta página web que suplanta a Sorel	
Alerta de seguridad cibernética	8FFR23-01240-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.botassorelcl[.]com/	
Dirección IP	
[196.242.16.249]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01240-01.txt	

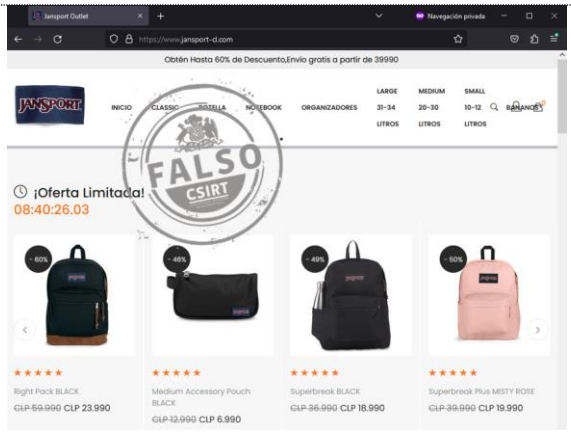


CSIRT alerta página web que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01241-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores 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_8FFR23-01241-01.txt	

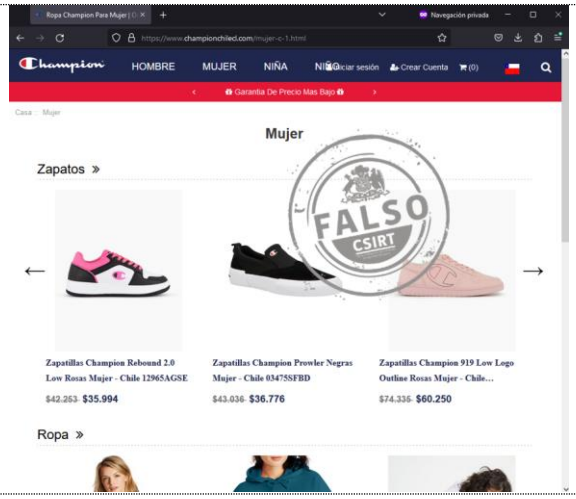


CSIRT advierte sitio que suplanta a Merrell	
Alerta de seguridad cibernética	8FFR23-01242-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.merrellchileofertas[.]com/	
Dirección IP	
[196.196.205.239]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01242-01.txt	

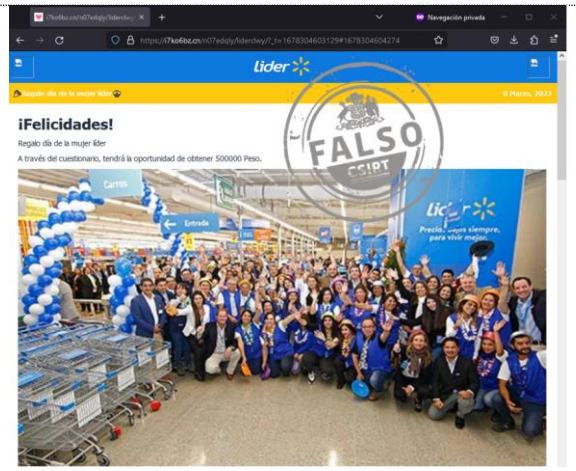
CSIRT alerta de página web que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01243-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2023
Última revisión	7 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://dev-aceptar-nuevo-aumento4.pantheonsite[.]io/	
Dirección IP	
[23.185.0.3]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01243-01.txt	



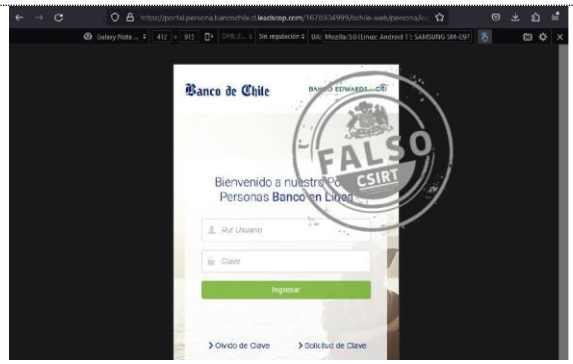
CSIRT alerta sitio web falso de JanSport	
Alerta de seguridad cibernética	8FFR23-01244-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2023
Última revisión	7 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.jansport-cl[.]com/	
Dirección IP	
[172.67.175.180]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01244-01.txt	



CSIRT advierte página web que suplanta a Champion	
Alerta de seguridad cibernética	8FFR23-01245-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.championchilecl[.]com/	
Dirección IP	
[196.245.249.87]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01245-01.txt	

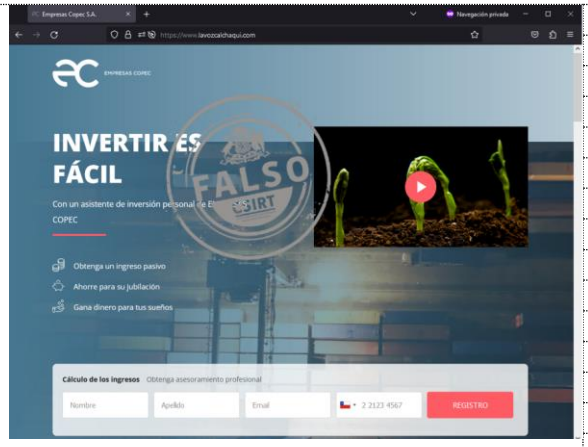


CSIRT alerta de sitio web falso de Líder	
Alerta de seguridad cibernética	8FFR23-01246-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
http://w.attractpant[.]cyou/0830al9_RUBERlRkW31kAxsHbFh9D0lYFQ1BNVIFMA0bXDQmaz4eFl0eEVs6HFMDSAkjekUgaAg6VAkgFAtEXR5eIQka?pngw1678303073349 https://i7ko6bz[.]cn/n07edqly/liderclwy/?_t=1678304603129#1678304604274	
Dirección IP	
[104.21.1.9]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01246-01.txt	



CSIRT informa de página web que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01247-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://is.gd/BancoChile https://portal.persona.bancochile.cl.leadscop[.]com/1678304999/bchile-web/persona/login/index.html/login	
Dirección IP	
[68.66.216.59]	

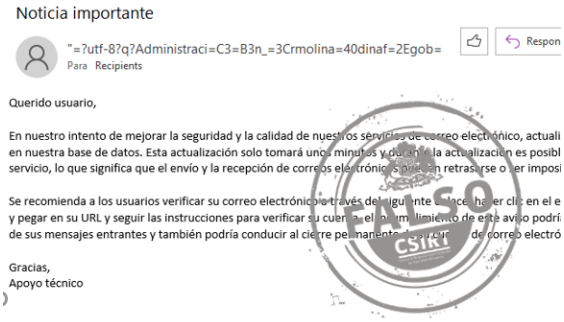
	Enlace para revisar IoC:
	https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01247-01.txt



CSIRT advierte sitio web falso que suplanta a Empresas Copec	
Alerta de seguridad cibernética	8FFR23-01248-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2023
Última revisión	9 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lavozcalchaqui[.]com/	
Dirección IP	
[172.67.203.208]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01248-01.txt	

2. Phishing

CSIRT alerta de campaña de smishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00764-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL redirección	
https[:]//contawebnwm[.]com/activacion/cuenta-wwnq/	
URL sitio falso	
https[:]//nwmepsonpatito[.]top/1678107788/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.173.125]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00764-01.txt	



CSIRT alerta campaña de smishing que suplanta un inicio de sesión de correo electrónico	
Alerta de seguridad cibernética	8FPH23-00765-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL redirección	
https://webcocentricen.wapka[.]co/	
URL sitio falso	
https://webcocentricen.wapka[.]co/	
Dirección IP	
[173.212.225.42]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00765-01.txt	

CSIRT advierte campaña de phishing que suplanta al Fonasa	
Alerta de seguridad cibernética	8FPH23-00766-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL redirección	
http://w.entrepreneurialdevastating.cn/8a44AXl4AFgBWn9ISnZDakdlLS10ZFwIAxJxd00yJTccLFMHaA0pXAMjNkM3XgdJAyp-	

	Byl1IRBWOh1rAXMAFG80SD4?ttye1678113459138
	URL sitio falso
	https://tmbkkq[.]cyou/ccGhZ80J/fonasawy/?_t=1678122603320#1678122605732
	Dirección IP
	[172.64.171.15]
	Enlace para revisar IoC:
	https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00766-01.txt

CSIRT informa campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00767-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2023
Última revisión	9 de marzo de 2023
Indicadores de compromiso	
URL redirección	
https://apply.mituniversity.edu[.]in/activacion/banca-en-linea/	
URL sitio falso	
https://underfilehomestado[.]top/1678193232/imagenes/_personas/home/default.asp	
Dirección IP	
[202.89.39.2]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00767-01.txt	

CSIRT alerta campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00768-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2023
Última revisión	9 de marzo de 2023
Indicadores de compromiso	
URL redirección	
https://containd3structible[.]com/activacion/cuenta-ffca/	
URL sitio falso	
https://nwmepsonpatito[.]club/1678367363/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.131.190]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00768-01.txt	

3. Malware

CSIRT advierte campaña de phishing con malware que suplanta a Servipag	
Alerta de seguridad cibernética	2CMV23-00403-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
Asunto	
Factura digital	
Correo de Salida	
facturaenlinea@network.org	
SHA256	
69e8f969f539a7673b1378aada96812cf0d53549c54a235934defcee7bd27356 9cf7217cbd0273f3a37595f7b7c4bb4991391e9932cf90745022e26907e768e7 43692365c8c951e8929283a345ecfc13a58356add60439bf4e7d103a6be2c2c5 0fee513762149b1a3f82dca25a5ef05ec542d1cda15891c5eb766c6466542e15 5f833d1638fb64058d7f968914255a9c90c8479e94512e152949b3cc6b8421be 4fc4833ed0036469d258c5d7fbfda93e19fa9a18cb1ddd601a22bc961de00765 98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b	
Enlace para revisar IoC:	
https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00403-01.txt	

4. Concientización

Ciberguía: Cómo protegerse en el mundo digital

Como parte de la conmemoración del Día Internacional de la Mujer compartimos una nueva ciberguia con consejos para protegernos al interactuar con el mundo digital. Puede ser vista en nuestro Linkedin: https://www.linkedin.com/feed/update/urn:li:activity:7039317403607957504.

Exitosa charla interactiva para funcionarios públicos sobre efectos del Decreto 273

Especialistas del CSIRT de Gobierno y la Unidad de Coordinación Nacional de Ciberseguridad compartieron ayer las implicancias del Decreto 273 sobre notificación de Incidentes de ciberseguridad con más de 150 encargados de diversos organismos públicos.

El CSIRT de Gobierno invita a charla de la Fundación Katy Summer este 14 de marzo

El CSIRT de Gobierno y la Fundación Katy Summer invitan a toda la comunidad a una charla online gratuita para hablar sobre el ciberacoso este 14 de marzo, en el marco del Día Nacional Contra el Ciberacoso, a las 9:30 horas.

Inscripciones: https://registro.interior.gob.cl/charla-ciberacoso

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.

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.

- Margarita Hermosilla Henríquez
- Jaime
- Leyla Mendoza
- Julián Arias Maetschl
- Bárbara Palacios Cabezas
- Fernando Flores Tobar
- Elizabeth Viviana Parra Cortez