CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 234

semana del 22 al 28 de diciembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

22

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

24

URL asociadas a sitios fraudulentos y campañas de phishing y malware

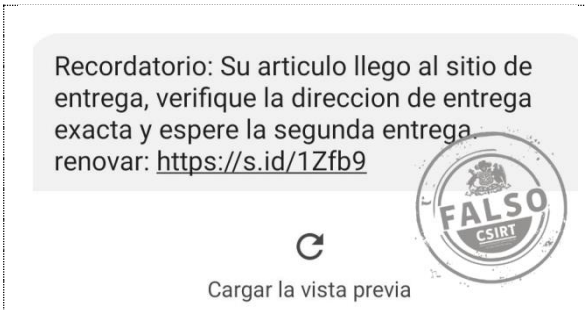
CONTENIDO

Contenido

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

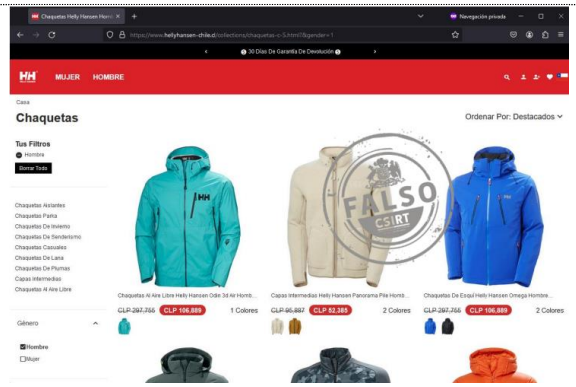
CSIRT alerta de campaña de phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH23-00916-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.glaucireis[.]com.br/1703251723/imagenes/_personas/home/default.asp	
URL de redirección	
https://procontroltotal[.]com/activacion/cuenta-ajwh/	
Dirección IP sitio falso	
[45.224.128.77]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph23-00916-01/	



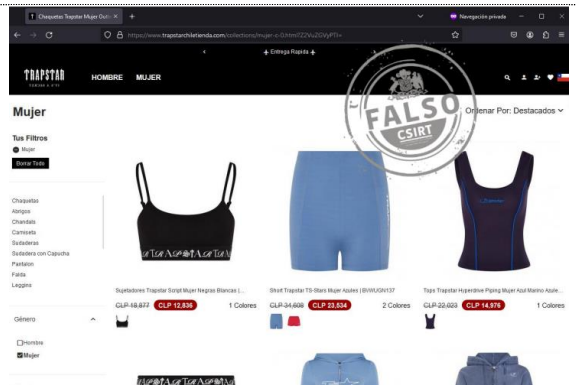
CSIRT alerta de campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00917-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 diciembre, 2023
Última revisión	27 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://clpotosenloy[.]info/	
URL de redirección	
https://s[.]id/1Zfb9	
Dirección IP sitio falso	
[170.106.158.50]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00917-01/	

CSIRT alerta de campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00918-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 diciembre, 2023
Última revisión	28 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.khansouq[.]com/1703773404/imagenes/_personas/home/default.asp	
URL de redirección	
https://www.cajaabogadossanjuan[.]org.ar/activacion/cuenta-acbv/	
Dirección IP sitio falso	
[199.188.200.192]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph23-00918-01/	

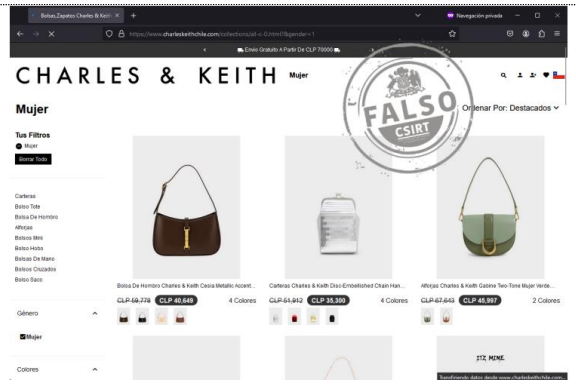
2. Sitios fraudulentos



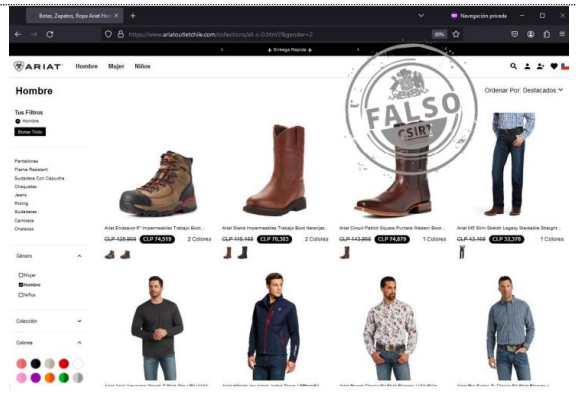
CSIRT advierte sitio falso que suplanta a Helly Hansen	
Alerta de seguridad cibernética	8FFR23-01610-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.hellyhansen-chile[.]cl/	
Dirección IP sitio falso	
[104.160.25.48]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01610-01/	



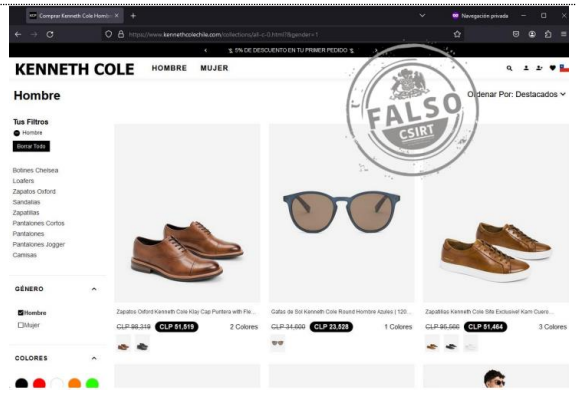
CSIRT advierte sitio falso que suplanta a Trapstar	
Alerta de seguridad cibernética	8FFR23-01611-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.trapstarchiletienda[.]com	
Dirección IP sitio falso	
[165.231.10.33]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01611-01/	



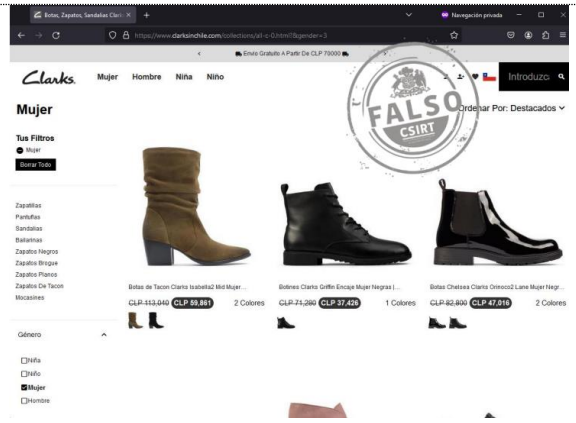
CSIRT advierte nuevo sitio falso que suplanta a Charles & Keith	
Alerta de seguridad cibernética	8FFR23-01612-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.charleskeithchile[.]com/	
Dirección IP sitio falso	
[196.245.158.179]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01612-01/	



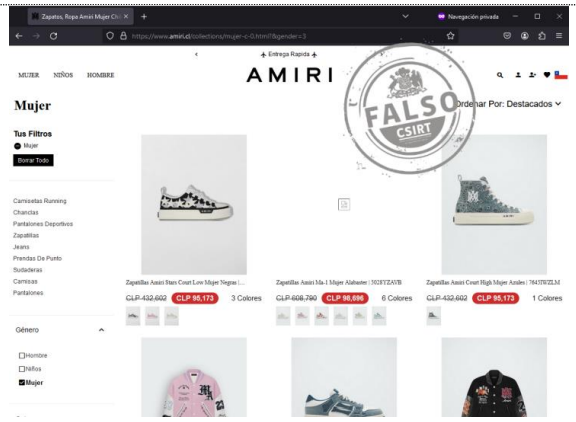
CSIRT advierte sitio falso que suplanta a Ariat	
Alerta de seguridad cibernética	8FFR23-01613-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.ariatoutletchile[.]com/	
Dirección IP sitio falso	
[196.196.206.141]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01613-01/	



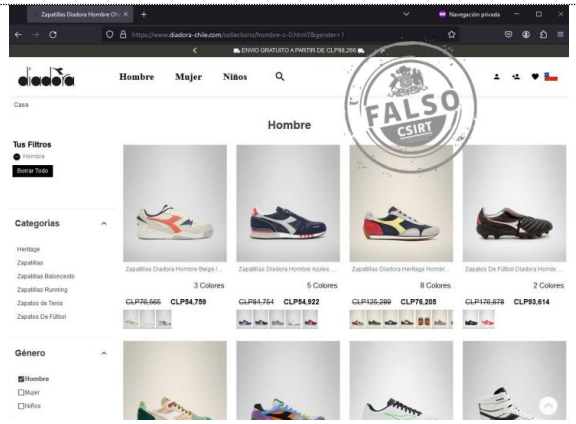
CSIRT advierte nuevo sitio falso que suplanta a Kenneth Cole	
Alerta de seguridad cibernética	8FFR23-01614-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.kennethcolechile[.]com	
Dirección IP sitio falso	
[196.196.12.163]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01614-01/	



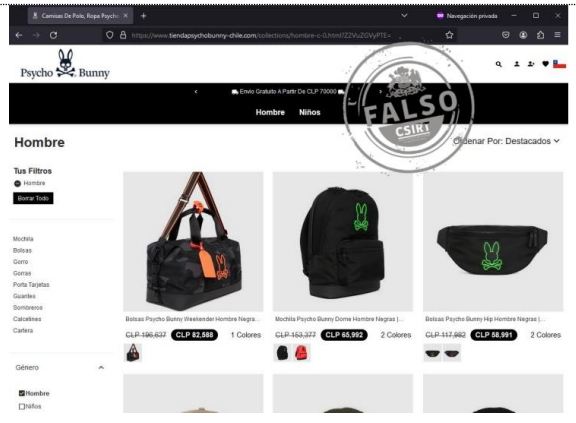
CSIRT advierte nuevo sitio falso que suplanta a Clarks	
Alerta de seguridad cibernética	8FFR23-01615-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.clarksinchile[.]com/	
Dirección IP sitio falso	
[196.196.231.118]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01615-01/	



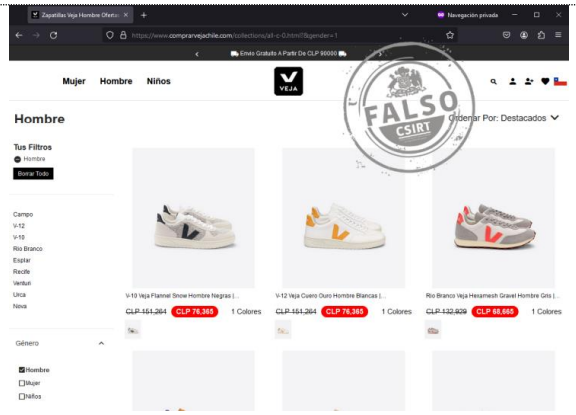
CSIRT advierte nuevo sitio falso que suplanta a Amiri	
Alerta de seguridad cibernética	8FFR23-01616-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.amiri[.]cl	
Dirección IP sitio falso	
[196.247.55.246]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01616-01/	



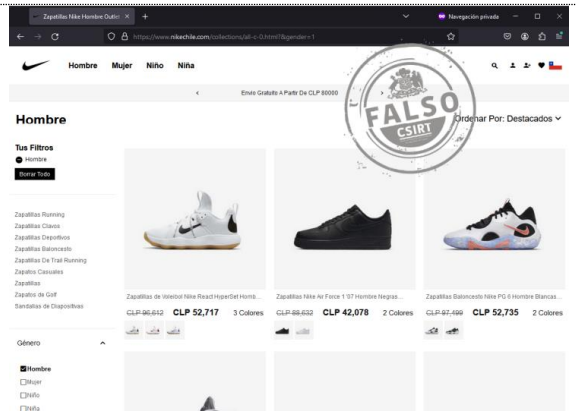
CSIRT advierte nuevo sitio falso que suplanta a Diadora	
Alerta de seguridad cibernética	8FFR23-01617-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.diadora-chile[.]com	
Dirección IP sitio falso	
[5.157.59.60]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01617-01/	



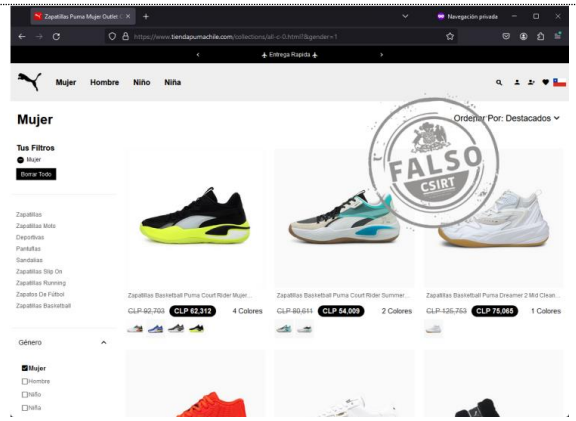
CSIRT advierte nuevo sitio falso que suplanta a Psycho Bunny	
Alerta de seguridad cibernética	8FFR23-01618-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.tiendapsychobunny-chile[.]com/	
Dirección IP sitio falso	
[104.160.4.67]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01618-01/	



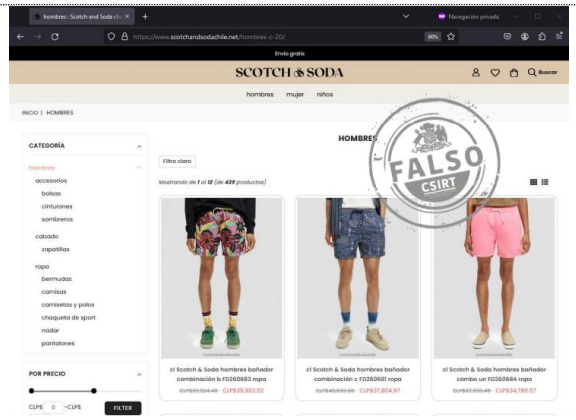
CSIRT advierte nuevo sitio falso que suplanta a Veja	
Alerta de seguridad cibernética	8FFR23-01619-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.comprarvejachile[.]com/	
Dirección IP sitio falso	
[196.196.197.78]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01619-01/	



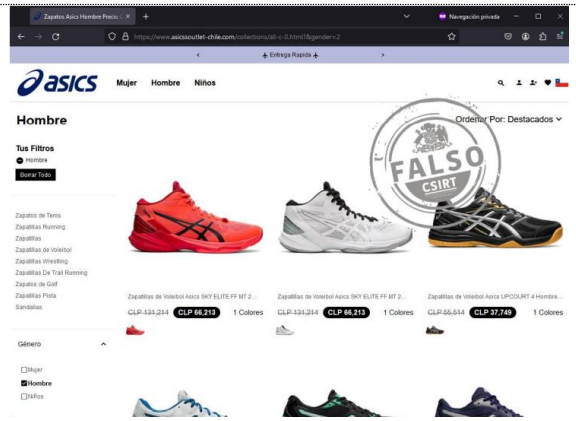
CSIRT advierte nuevo sitio falso que suplanta a Nike	
Alerta de seguridad cibernética	8FFR23-01620-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 diciembre, 2023
Última revisión	22 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.nikechile[.]com	
Dirección IP sitio falso	
[196.196.13.198]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01620-01/	



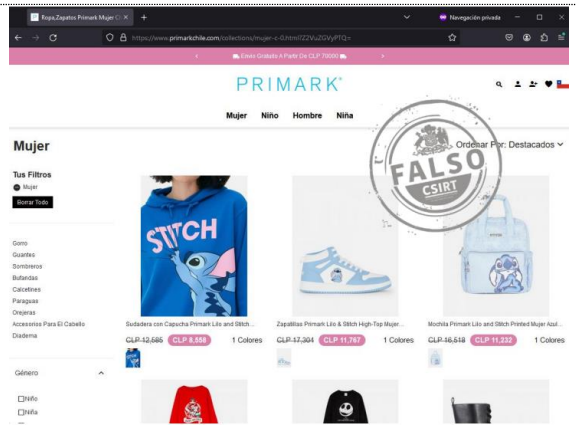
CSIRT advierte nuevo sitio falso que suplanta a Puma	
Alerta de seguridad cibernética	8FFR23-01621-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 diciembre, 2023
Última revisión	26 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.tiendapumachile[.]com	
Dirección IP sitio falso	
[196.196.197.170]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01621-01/	



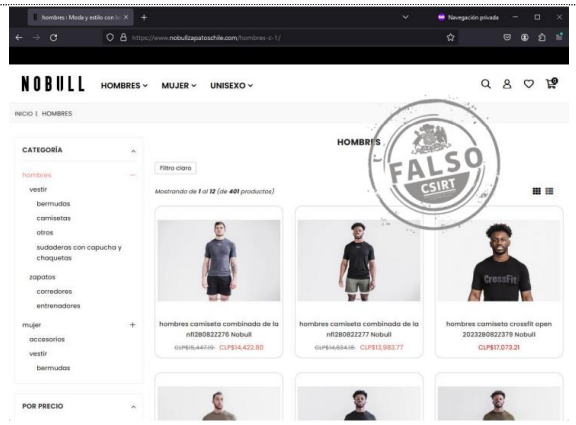
CSIRT advierte nuevo sitio falso que suplanta a Scotch & Soda	
Alerta de seguridad cibernética	8FFR23-01622-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 diciembre, 2023
Última revisión	26 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.scotchandsodachile[.]net	
Dirección IP sitio falso	
[104.21.45.80]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01622-01/	



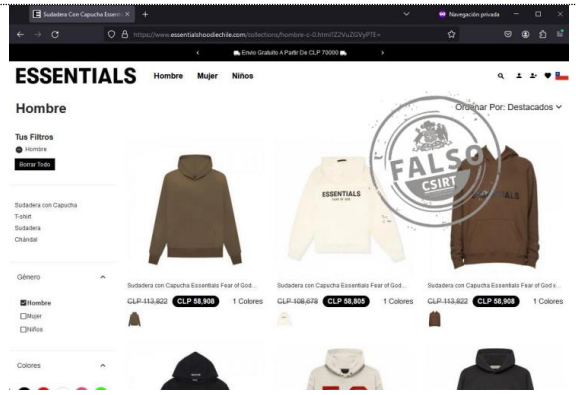
CSIRT advierte nuevo sitio falso que suplanta a Asics	
Alerta de seguridad cibernética	8FFR23-01623-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 diciembre, 2023
Última revisión	26 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.asicssoutlet-chile[.]com	
Dirección IP sitio falso	
[5.157.59.41]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01623-01/	



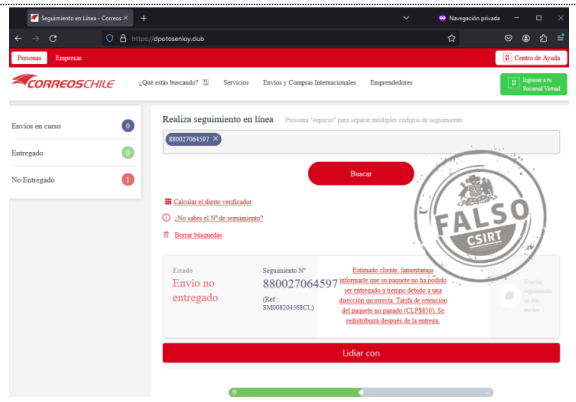
CSIRT advierte nuevo sitio falso que suplanta a Primark	
Alerta de seguridad cibernética	8FFR23-01624-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 diciembre, 2023
Última revisión	26 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.primarkchile[.]com	
Dirección IP sitio falso	
[196.198.12.105]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01624-01/	



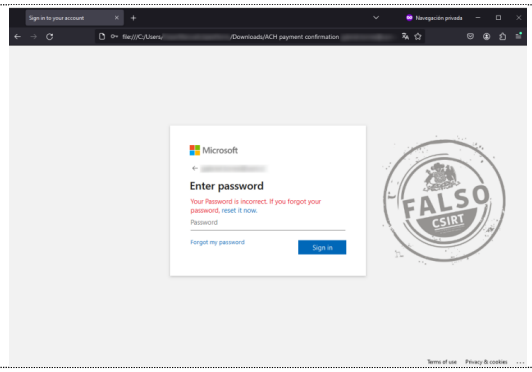
CSIRT advierte nuevo sitio falso que suplanta a No Bull	
Alerta de seguridad cibernética	8FFR23-01625-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 diciembre, 2023
Última revisión	26 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.nobullzapatoschile[.]com	
Dirección IP sitio falso	
[196.244.195.19]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01625-01/	



CSIRT advierte nuevo sitio falso que suplanta a Essentials	
Alerta de seguridad cibernética	8FFR23-01626-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 diciembre, 2023
Última revisión	27 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://essentialshoodiechile[.]com/	
Dirección IP sitio falso	
[196.196.192.136]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01626-01/	



CSIRT advierte nuevo sitio falso que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01627-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 diciembre, 2023
Última revisión	27 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://clpotosenloy[.]club/	
Dirección IP sitio falso	
[170.106.158.50]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01627-01/	



CSIRT advierte nuevo sitio falso que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR23-01628-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 diciembre, 2023
Última revisión	28 diciembre, 2023
Indicadores de compromiso	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01628-01/	

3. 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.

4. 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.

- Andrea Baccelliere
- Waldemar Waller
- Francisco Jiménez
- Orlando Navarrete
- Marcelo Araneda
- Felipe Hernández

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.12.29 11:20:22 -03'00'