CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 244

semana del 1 al 7 de marzo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

11

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

14

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

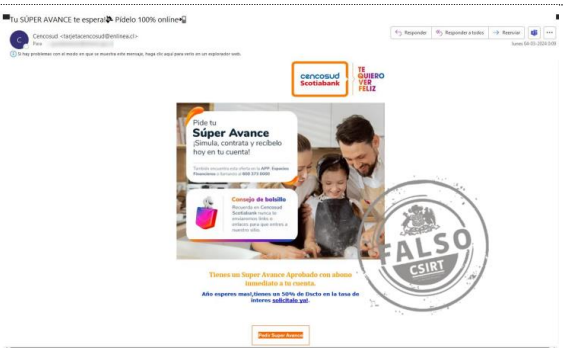
4

Las mitigaciones son útiles en productos Cisco

CONTENIDO

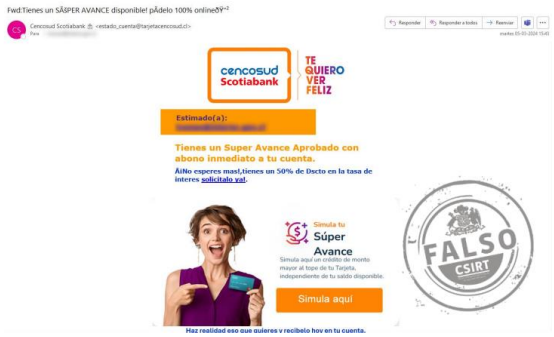
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing



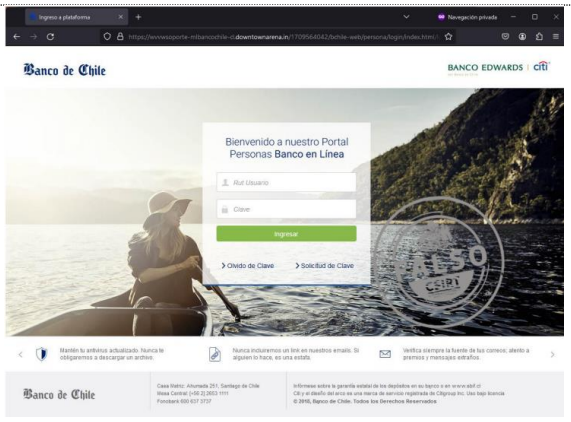
CSIRT alerta de campaña de phishing que suplanta a Cencosud Scotianbank	
Código de alerta	8FPH24-00936-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo, 2024
Última revisión	4 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://mitarjetacencosud-cl-mitarjetacencosud-cl-mitarjetacencosud-cl.aumentos-chile-cl[.]life/1709563097/login/index.html	
URL de redirección	
https://mitarjetacencosud-cl-mitarjetacencosud-cl-mitarjetacencosud-cl.aumentos-chile-cl[.]life/1709563097/login/index.html	
Dirección IP sitio falso	
[104.21.47.4]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00936-01/	

CSIRT alerta de campaña de phishing sobre caducidad de cuenta de correo	
Código de alerta	8FPH24-00937-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo, 2024
Última revisión	4 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://profile.classers.shop/administration.html?mail={mail}	
URL de redirección	
https://linkedin.com+accounts%3Dsecurelogin+settings%3Dprivate@profile.classers.shop/administration.html?mail={mail}	
Dirección IP sitio falso	
[172.67.169.242]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00937-01/	

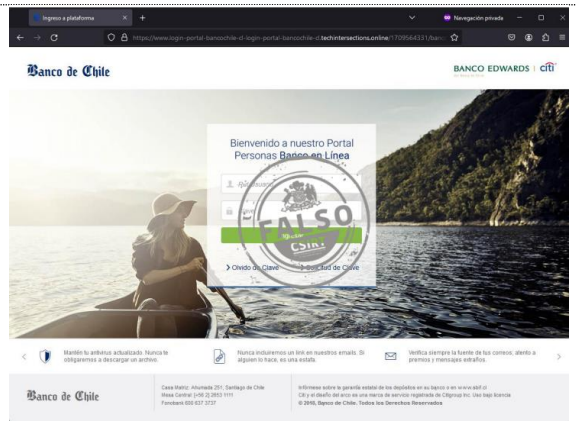


CSIRT alerta de campaña de phishing que suplanta a Cencosud Scotianbank	
Código de alerta	8FPH24-00938-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo, 2024
Última revisión	6 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://mi-tarjetacencosud-cl.itsdjlucky[.]com/	
URL redirección	
https://sam-tech[.]jp/cencosud/superavance-jqes/	
Dirección IP sitio falso	
[62.210.114.93]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00938-01/	

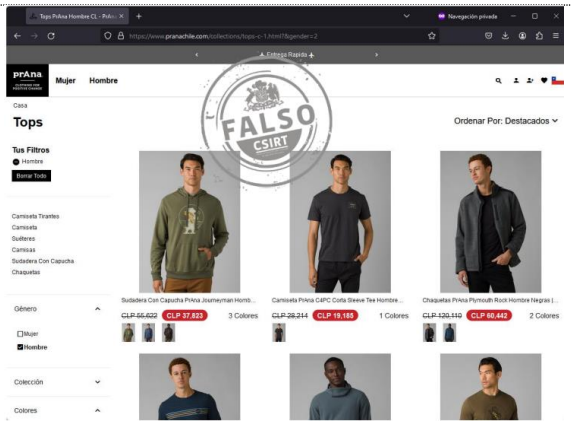
2. Sitios fraudulentos



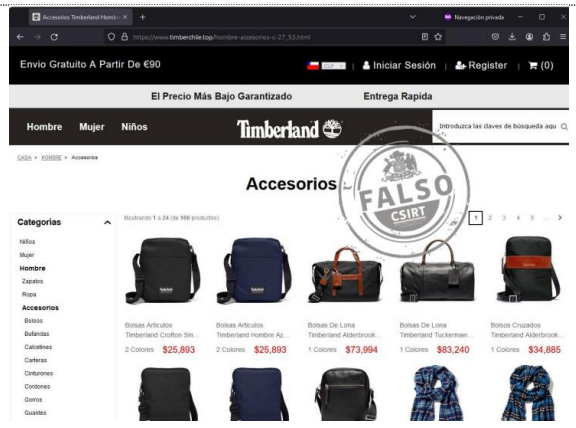
CSIRT advierte nuevo sitio falso que suplanta al Banco de Chile	
Código de alerta	8FFR23-01655-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de marzo, 2024
Última revisión	1 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://wvvwsoporte-mlbancochile-cl.downtownarena[.]in/1709564042/bchile-web/persona/login/index.html/login	
Dirección IP sitio falso	
[216.137.176.69]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01655-01/	



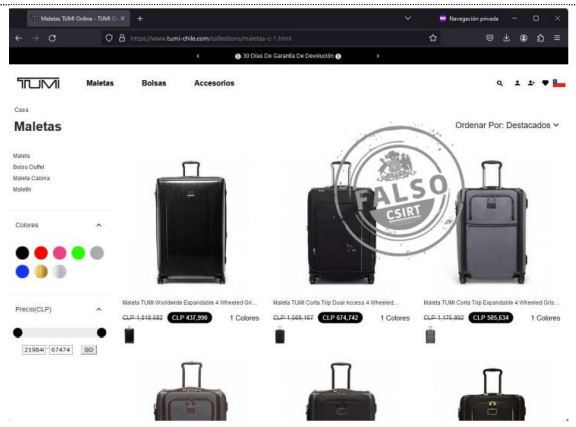
CSIRT advierte nuevo sitio falso que suplanta al Banco de Chile	
Código de alerta	8FFR23-01656-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo, 2024
Última revisión	4 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.login-portal-bancochile-cl-login-portal-bancochile-cl.techintersections[.]online/1709564331/bancochile-web/persona/login/index.html/login	
Dirección IP sitio falso	
[43.250.249.65]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01656-01/	



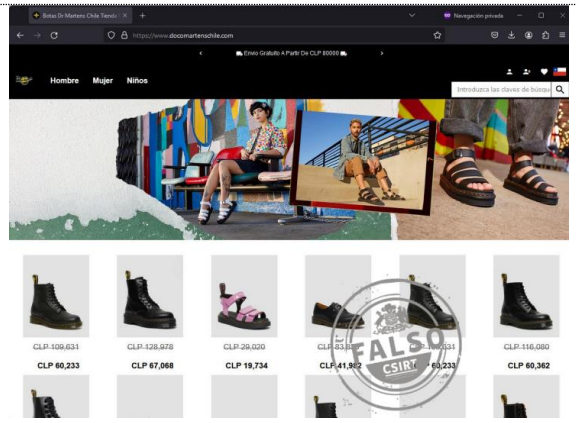
CSIRT advierte nuevo sitio falso que suplanta a Prana	
Código de alerta	8FFR23-01657-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de marzo, 2024
Última revisión	5 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.pranachile[.]com	
Dirección IP sitio falso	
[196.196.38.155]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01657-01/	



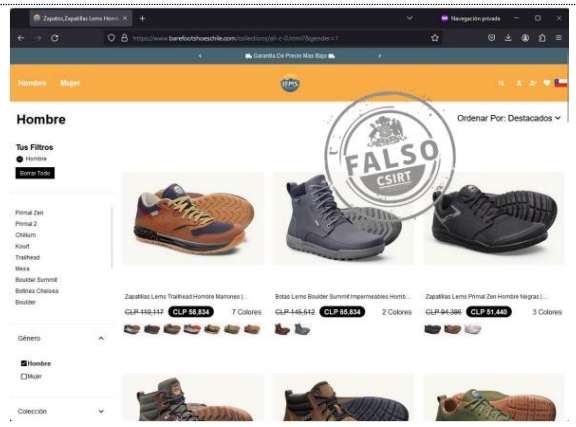
CSIRT advierte nuevo sitio falso que suplanta a Timberland	
Código de alerta	8FFR23-01658-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de marzo, 2024
Última revisión	5 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.timberchile[.]top/	
Dirección IP sitio falso	
[196.242.16.134]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01658-01/	



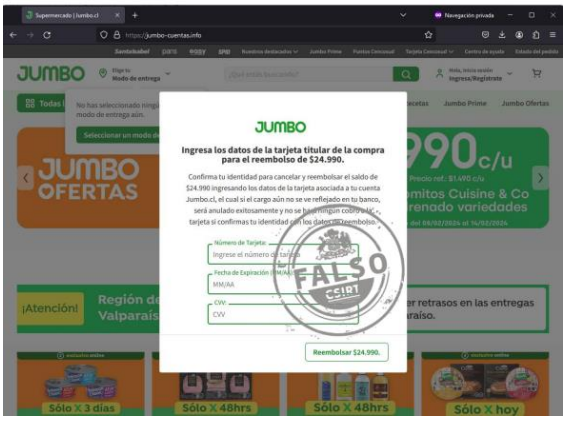
CSIRT advierte nuevo sitio falso que suplanta a Tumi	
Código de alerta	8FFR23-01659-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de marzo, 2024
Última revisión	5 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.tumi-chile[.]com	
Dirección IP sitio falso	
[165.231.191.230]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01659-01/	



CSIRT advierte nuevo sitio falso que suplanta a Dr. Martens	
Código de alerta	8FFR23-01660-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de marzo, 2024
Última revisión	5 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.docomartenschile[.]com/	
Dirección IP sitio falso	
[196.196.38.97]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01660-01/	



CSIRT advierte nuevo sitio falso que suplanta a Lems	
Código de alerta	8FFR23-01661-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo, 2024
Última revisión	6 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.barefootshoeschile[.]com	
Dirección IP sitio falso	
[165.231.153.31]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr24-01661-01/	



CSIRT advierte nuevo sitio falso que suplanta a Jumbo	
Código de alerta	8FFR23-01662-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo, 2024
Última revisión	6 de marzo, 2024
Indicadores de compromiso	
URL del sitio falso	
https://uchilecl.weebly[.]com/	
Dirección IP sitio falso	
[199.34.228.53]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr24-01662-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades que afectan a VMware ESXi, Workstation y Fusion	
Código de alerta	9VSA24-00981-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo, 2024
Última revisión	6 de marzo, 2024
CVE	
CVE-2024-22252 CVE-2024-22253 CVE-2024-22254 CVE-2024-22255	
Fabricante	
VMware	
Productos afectados	
VMware ESXi VMware Workstation Pro / Reproductor (estación de trabajo) VMware Fusion Pro / Fusion (Fusión) VMware Cloud Foundation (Fundación en la nube)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00981-01/	

4. Malware

CSIRT advierte phishing con malware que suplanta al Servicio de Impuestos Internos	
Código de alerta	2CMV24-00448-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de marzo, 2024
Última revisión	1 de marzo, 2024
Indicadores de compromiso	
SHA256	
657755a59be263e7cf3a5b2d769a276a06e60c6f7ddeab579141b14508d8b43b	
126c90a8396077de034acf0a4a38927ec3d807533e6e2c247807ccebfec5da28	
e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/2cmv24-00448-01/	

CSIRT advierte phishing con malware con una falsa demanda	
Código de alerta	2CMV24-00449-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de marzo, 2024
Última revisión	4 de marzo, 2024
Indicadores de compromiso	
SHA256	
571c694a88a7187135e203990af43edcab1234406d3ffe964b60b0aa26b4060b	
a74b87754eb9a6a7e6b19da79eb02192b6e1a802fe58d037065a33ac7171f57d	
f2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59	
013dbfa17653c4fc89a20f7c988bdfb6b5c3367a0c6a8e3a87e189e164e53460	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/2cmv24-00449-01/	

5. Noticias y concientización

Ciberconsejos | Uso responsable de Tik Tok e Instagram

De acuerdo a un estudio elaborado por Kaspersky llamado "Niños Digitales", el 55% de los menores chilenos tiene alguna cuenta en Redes Sociales. ¿Sabes cómo ayudar a tus hijos a usar estas plataformas de forma responsable? Aquí te entregamos algunos tips sobre Instagram y Tik Tok para proteger a tus hijos.

6. 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.

7. 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.

- Francisco Flefil
- Mathias Roco
- Héctor Prieto
- Diego Grande
- Carlos Escalona
- Diego Concha

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.03.08 16:51:43 -03'00'