CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 199

semana del 21 al 27 de abril de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

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

URL ADVERTIDAS

24 URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

8 Las mitigaciones son útiles en productos de SolarWinds y VMware.

HASH REPORTADOS

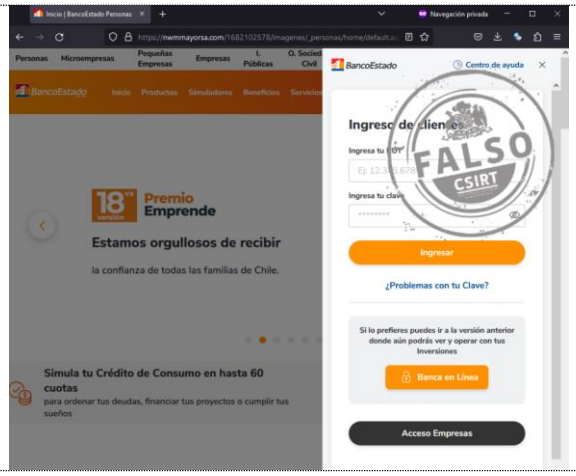
4 asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

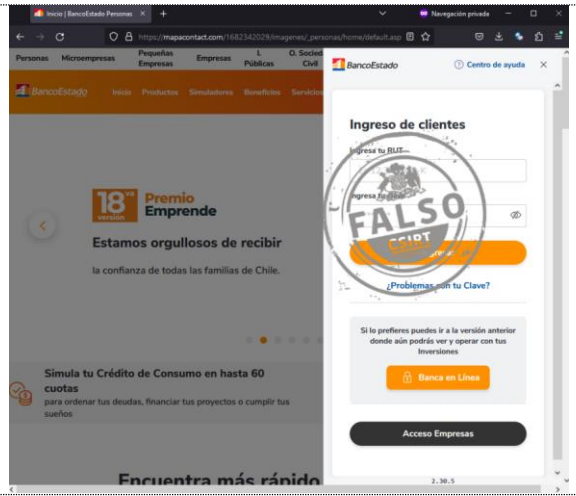
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

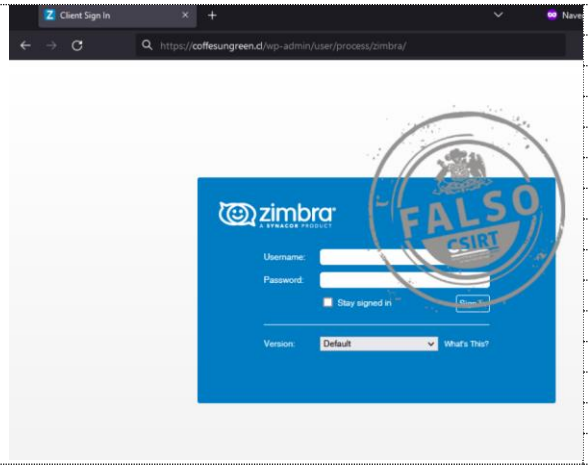
CSIRT alerta de página fraudulenta que suplanta a Colloky	
Alerta de seguridad cibernética	8FFR23-01293-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]clothingfactorys.weebly.com/ https[:]//www.vetemcam.online/	
Dirección IP	
[167.160.3.13]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01293-01	



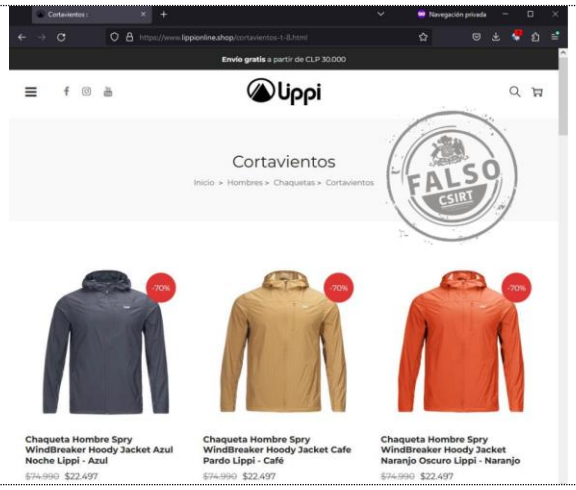
CSIRT alerta de sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01294-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//nwmmayorsa.com/1682102578/imagenes/_personas/home/default.asp	
Dirección IP	
[67.23.242.202]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01294-01	



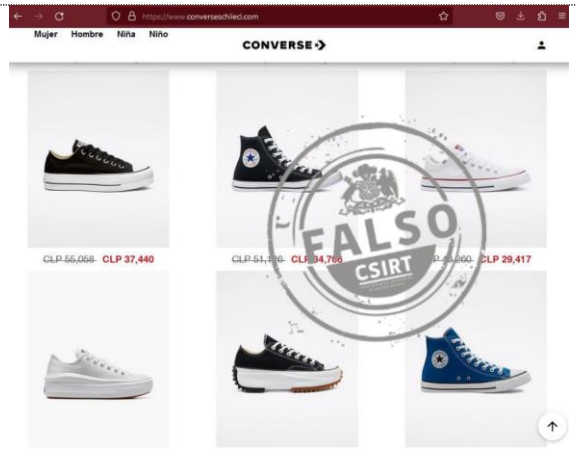
CSIRT alerta de página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01295-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//mapacontact[.]com/1682342029/imagenes/_personas/home/default.asp	
Dirección IP	
[72.29.91.210]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01295-01	



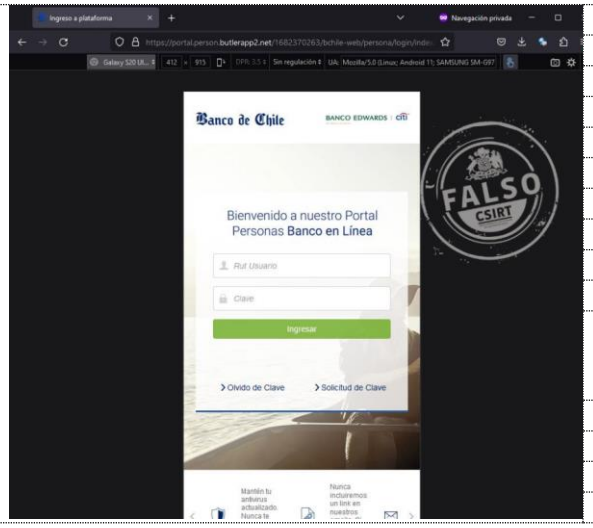
CSIRT alerta de nueva página fraudulenta que suplanta a Zimbra	
Alerta de seguridad cibernética	8FFR23-01296-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//coffesungreen[.]cl/wp-admin/user/process/zimbra/	
Dirección IP	
[190.196.214.221]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01296-01	



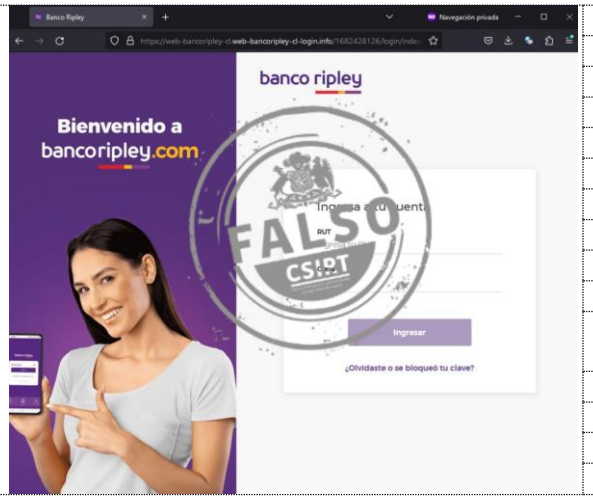
CSIRT alerta ante nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01297-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.lippionline[.]shop/	
Dirección IP	
[172.67.221.142]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01297-01	



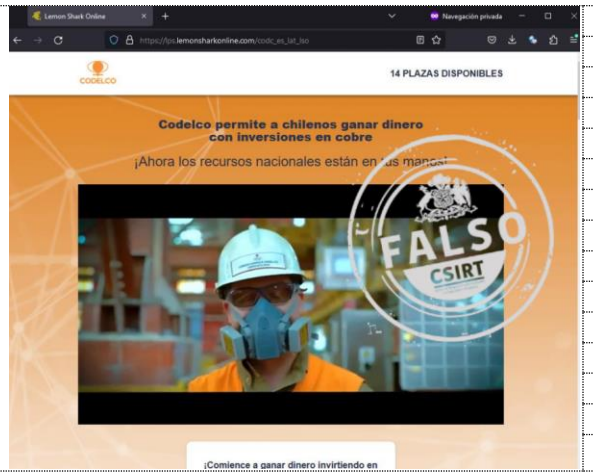
CSIRT alerta de sitio fraudulento que suplanta a Converse	
Alerta de seguridad cibernética	8FFR23-01298-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.converseschilecl.com/	
Dirección IP	
[196.247.29.14]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01298-01	



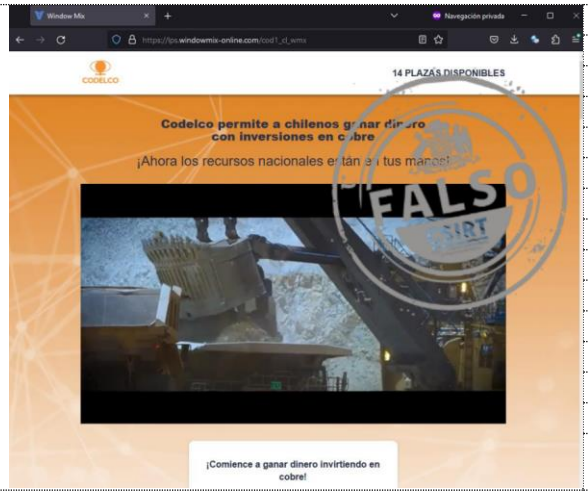
CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01299-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//is[.]gd/AyudaBancoChile https[:]//portal.person.butlerapp2[.]net/1682370263/bchile-web/persona/login/index.html/login	
Dirección IP	
[68.66.216.52]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01299-01	



CSIRT alerta de sitio fraudulento que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01300-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web-bancoripley-cl.web-bancoripley-cl-login.info/1682428126/login/index.html	
Dirección IP	
[172.64.80.1]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01300-01	

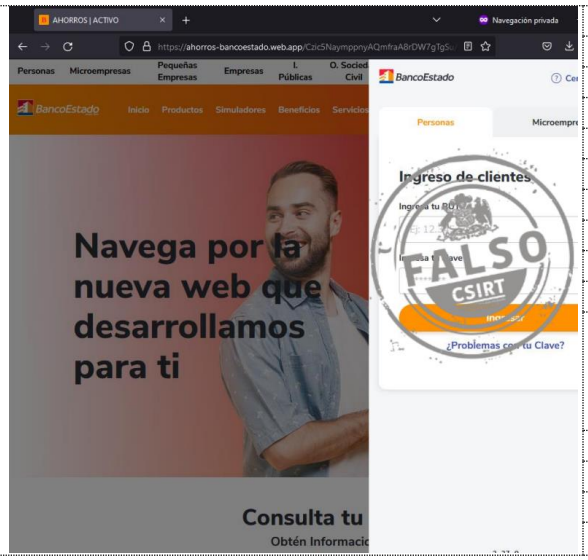


CSIRT alerta de sitio fraudulento que suplanta a Codelco	
Alerta de seguridad cibernética	8FFR23-01301-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//lps.lemonsharkonline[.]com/codc_es_lat_lso	
Dirección IP	
[104.21.53.39]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01301-01	



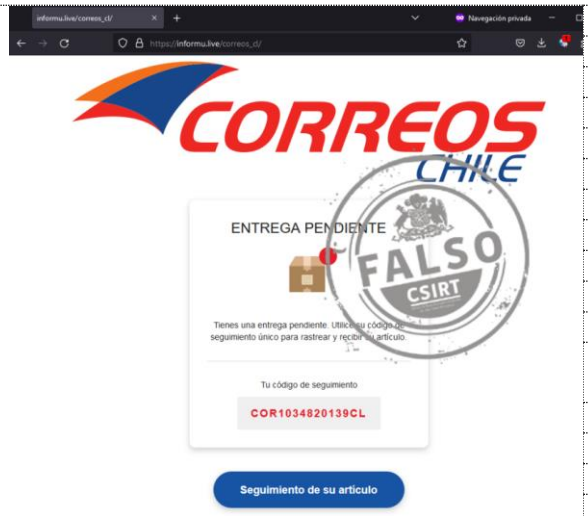
CSIRT alerta ante sitio fraudulento que suplanta a Codelco	
Alerta de seguridad cibernética	8FFR23-01302-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//lps.windowmix-online[.]com/cod1_cl_wmx	
Dirección IP	
[172.67.165.248]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01302-01	

CSIRT advierte ante nueva página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01303-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//p0rtalpersons-bnncochile.cl-sow[.]top/1682458068/bchile-web/persona/login/index.html/login	
Dirección IP	
[104.21.57.217]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01303-01	

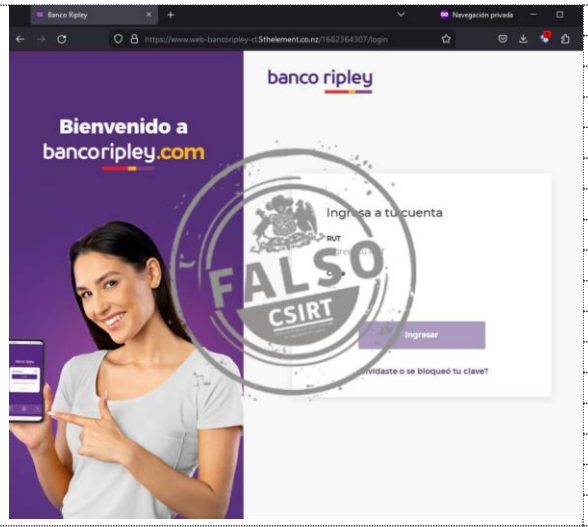


CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01304-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//bit[.]ly/40wP5AM https[:]//ahorros-bancoestado.web[.]app/btCXLHfcDNukkZqUaL9TrbtdBY9xqA/itm?source=true&pf_rd_r=hjdfdl67bjk	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01304-01	

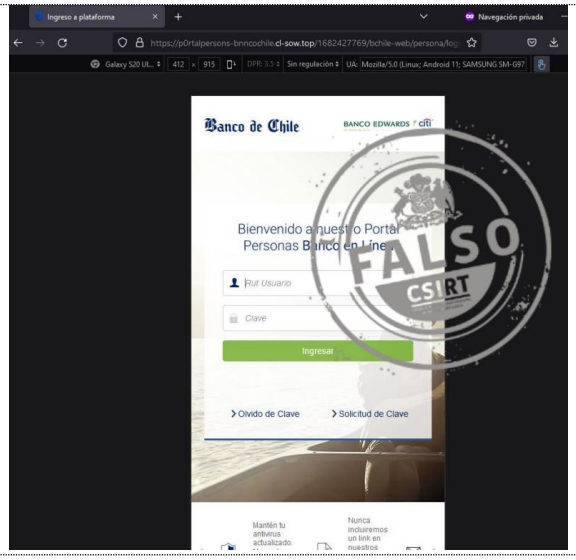
2. Phishing



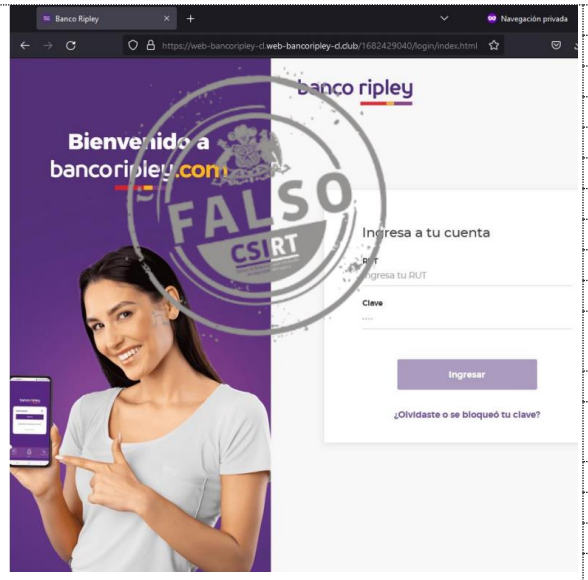
CSIRT alerta ante campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00797-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
URL redirección	
http[:]//cuqd[.]me/Zs1ucE	
URL sitio falso	
https[:]//informu[.]live/correos_cl/ https[:]//fndngsmnspcltdy.com/user	
Dirección IP	
[93.95.227.126]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00797-01/	



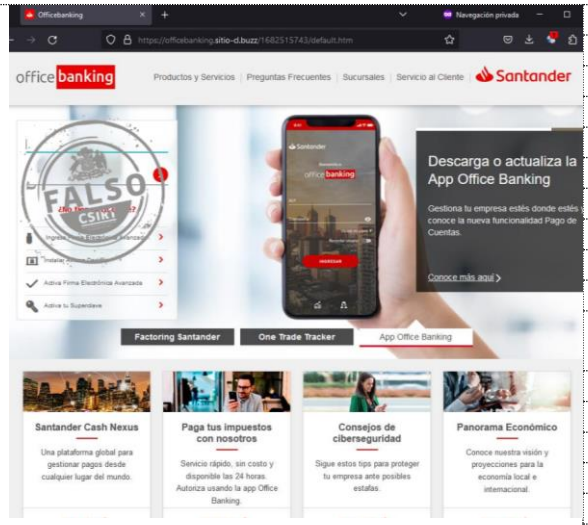
CSIRT alerta campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00798-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.web-bancoripley-cl.5thelement[.]co.nz/1682364307/login	
URL redirección:	
https[:]//bit[.]ly/40tvcd7?l=www.bancoripley.cl	
Dirección IP sitio falso	
[185.184.154.1]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00798-01/	



CSIRT alerta ante nueva campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH23-00799-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//p0rtalpersons-bnncochile.cl-sow[.]top/1682427635/bchile-web/persona/login/index.html/login	
URL redirección:	
https[:]//bit[.]ly/3N6INUQ	
Dirección IP sitio falso	
[104.21.57.217]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00799-01/	



CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00800-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
Indicadores de compromiso	
URL redirección:	
https[:]//bit[.]ly/40B3Hyg?l=www.bancoripley.cl https[:]//sam-tech[.]jp/bancoripley/cuenta-wplw/	
URL sitio falso:	
https[:]//web-bancoripley-cl.web-bancoripley-cl[.]club/1682429040/login/index.html	
Dirección IP sitio falso	
[104.21.17.239]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00800-01/	



CSIRT alerta de una nueva campaña de phishing que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00801-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//bit[.]ly/3HgiyYp?l=www.officebanking.cl http[:]//wordpress.zuliatec.com[.]ve/activacion/cuenta-ufbq/	
URL sitio falso	
https[:]//officebanking.sitio-cl[.]buzz/1682515743/default.htm	
Dirección IP	
[172.67.212.81]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00801-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades críticas para VMware Aria Operations for Logs	
Alerta de seguridad cibernética	9VSA23-00821-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023
CVE	
CVE-2023-20864 CVE-2023-20865	
Fabricantes	
VMware	
Productos afectados	
VMware Aria Operations for Logs	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00821-01/	

CSIRT comparte información de vulnerabilidades parchadas en SolarWinds Platforms	
Alerta de seguridad cibernética	9VSA23-00822-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
CVE	
CVE-2022-36963 CVE-2022-47505 CVE-2022-47509 CVE-2023-23838 CVE-2023-23837	
Fabricantes	
Solarwinds	
Productos afectados	
SolarWinds Platform, versiones anteriores a la 2023.2, que resuelve ambas vulnerabilidades.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00825-01/	

CSIRT comparte vulnerabilidad crítica parchada por VMware	
Alerta de seguridad cibernética	9VSA23-00823-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2023
Última revisión	27 de abril de 2023
CVE	
CVE-2023-20869	
Fabricantes	
VMware	
Productos afectados	
VMware Workstation y Fusion. Versiones corregidas: Workstation 17.0.2 y Fusion 13.0.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00823-01/	

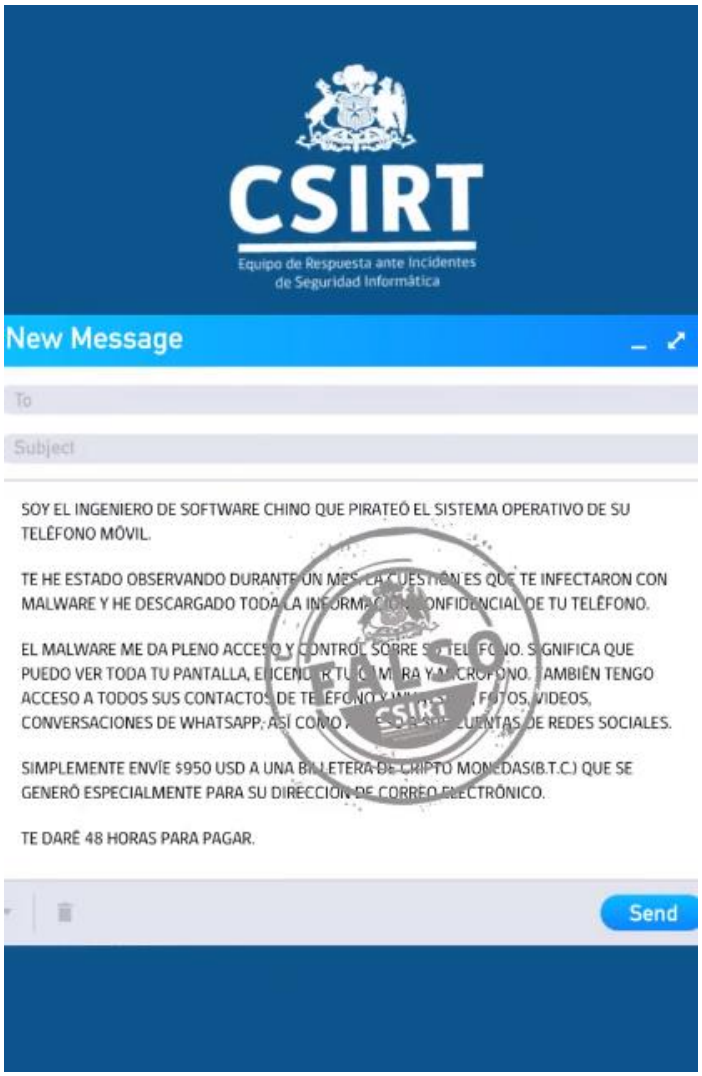
4. Malware

CSIRT alerta de nueva campaña de phishing con malware, que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV23-00411-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023
Indicadores de compromiso	
URL-Dominio	
bazuca20233.hopto[.]org	
SHA256	
f1b1e0e27582995da9cf2c9545a41b18a3d4397b9e24cfc981f50ab0e20461e2 de87c8713fac002b0b0a0f9b02c4e3ebcccf65282a22f5ab5912a9da00f35c2a fe2b187f223d323379ff82e2f561ec3b559e6422166800debf2d192d5cd8cb56 c09d0790e550694350b94ca6b077c54f983c135fab8990df5a75462804150912	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00411-01/	

5. Concientización

Advertencia email de phishing

Esta semana alertamos a la comunidad, a través de nuestros Instagram y Twitter de CSIRT Conciencia, de un correo maliciso que simulaba provenir de un supuesto hacker chino, y que extorsionaba a sus receptores amenazando que si no era pagado publicaría fotos privadas de ellos. Pueden verlo aquí: https://twitter.com/CSIRTConciencia/status/1650608697058492416?s=20.



Ciberdiccionario Volumen 34

En la presente edición del Ciberdiccionario decidimos incluir dos situaciones, el grooming y la sextorsión, que, de sufrirlas, pueden ser denunciados a la Policía de Investigaciones (PDI) y el Ministerio Público. Además, revisamos el single sign-on y los ataques BEC. Como siempre, está disponible también en el siguiente link: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-34/.

Ciberconsejos para cuidar tu ClaveÚnica

La ClaveÚnica es la forma que tienes para acceder a los servicios del Estado de forma online y realizar diversos trámites, por eso nunca debes entregar tus datos de ClaveÚnica a ninguna institución ni persona, ya que podrías ser víctima de un mal uso o de algún fraude. ¡Sólo tú eres el dueño de esa información!

El CSIRT de Gobierno junto con Gobierno Digital lanzamos una campaña con las siguientes recomendaciones: csirt.gob.cl/recomendaciones/ciberconsejos-para-cuidar-tu-claveunica/

BEC | Ciberincidentes en niveles directivos y de gestión crítica

Una forma en la que los ciberdelincuentes buscan causar el mayor daño a empresas y otras instituciones es enfocándose en engañar a personas en los niveles directivos y de gestión crítica de las organizaciones. Estos ataques, entre los que se encuentran el BEC, o compromiso de correo empresarial, y el Fraude del CEO.

En el siguiente enlace les explicamos las características de los principales ataques contra los niveles directivos y de gestión crítica, y cómo darnos cuenta de que podemos estar en presencia de alguno de ellos, para evitar ser una víctima: https://www.csirt.gob.cl/recomendaciones/bec-2023/.

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.

- Andres Santana Mansilla
- Cristian Navarrete
- Claudio Soto
- Wladimir Hernandez
- Juan Carlos Molina
- Tamara Llaneza
- Isabel Alejandra González
- Julio López Rodríguez
- Raúl Yañez Belmar
- Jorge Alejandro Ramos
- Oscar Rodrigo Ulloa
- Ximena Pérez

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.28 16:38:11 -04'00'