CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 208

semana del 23 al 29 de junio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

21

IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

44

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

5

Las mitigaciones son útiles en productos de Apple y Fortinet.

HASH REPORTADOS

9

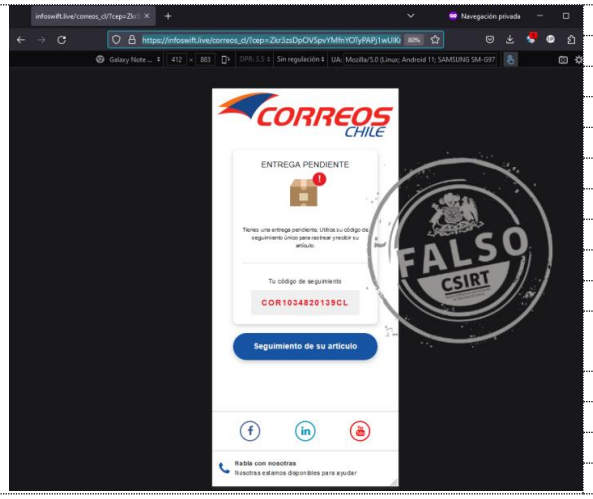
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

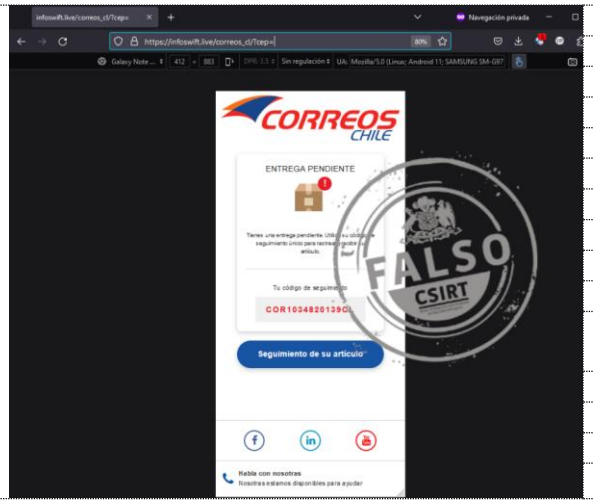
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

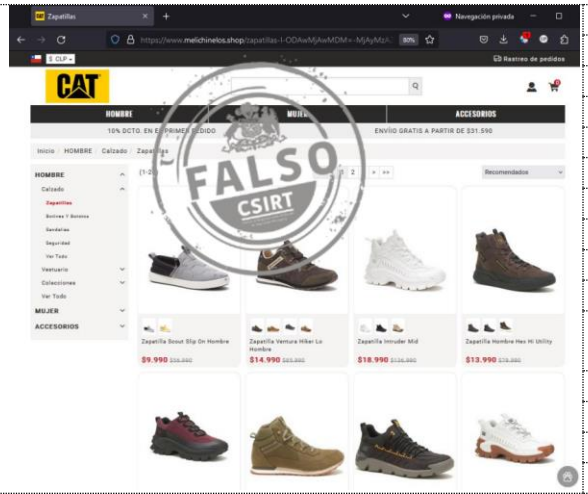
CSIRT alerta de sitio fraudulento de ventas falsas, denominado Gipso Shop	
Alerta de seguridad cibernética	8FFR23-01420-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://gipsochile[.]com/	
Dirección IP	
[23.227.38.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01420-01	



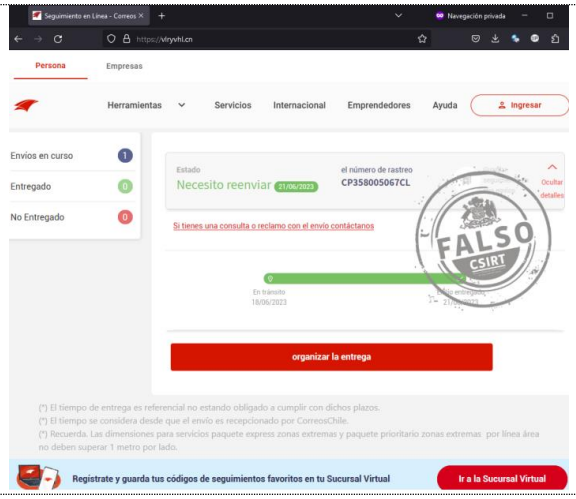
CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01421-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
http://tsqm[.]me/Zerz4a https://infoswift[.]live/correos_cl/?cep=	
Dirección IP	
[93.95.225.248]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01421-01/	



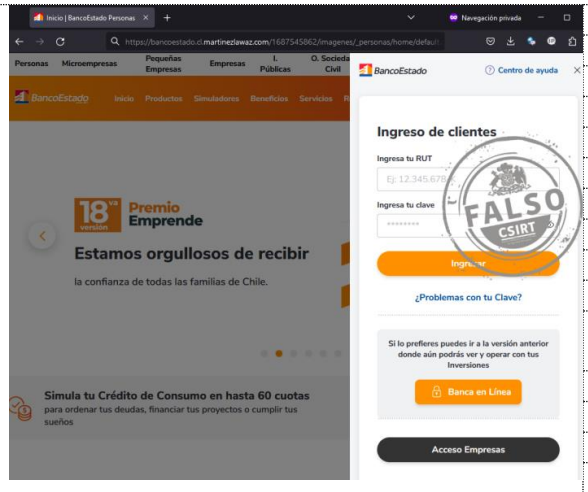
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01422-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
http://xmmh[.]me/Zeqbmv https://infoswift[.]live/correos_cl/?cep=	
Dirección IP	
[93.95.225.248]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01422-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01423-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://catclshop.my[.]canva.site/ https://www.melichinelos[.]shop	
Dirección IP	
[107.150.173.210]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01423-01/	

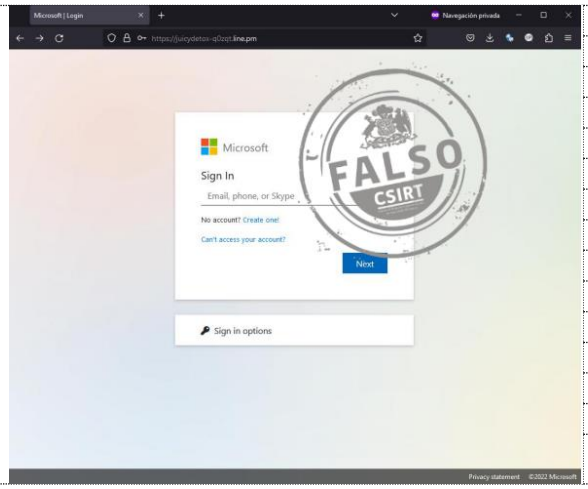


CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01424-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://is[.]gd/kyurSE https://vlryvhl[.]cn/	
Dirección IP	
[204.44.66.63]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01424-01/	

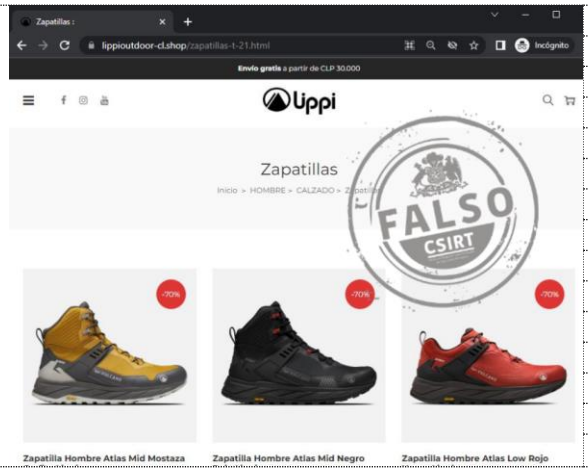


CSIRT alerta ante sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01425-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://bancoestado.cl.martinezlawaz[.]com/1687545862/imagenes/_personas/ home/default.asp	
Dirección IP	
[50.87.145.149]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01425-01/	

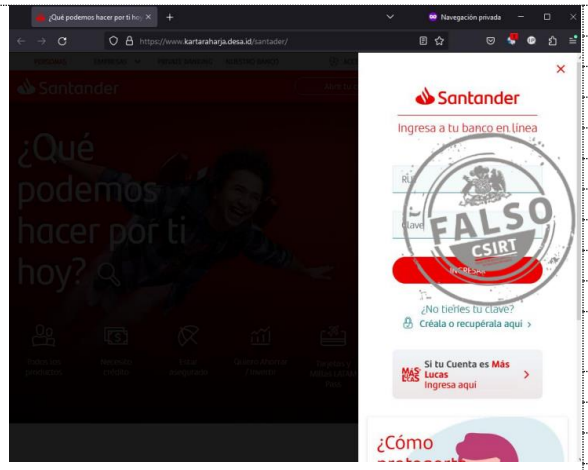
CSIRT alerta ante nuevo sitio fraudulento que suplanta a CCU	
Alerta de seguridad cibernética	8FFR23-01426-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://lps.lemonshark-online[.]com/ucc_5305_1_es_lat_lso/	
Dirección IP	
[104.21.40.194]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01426-01/	



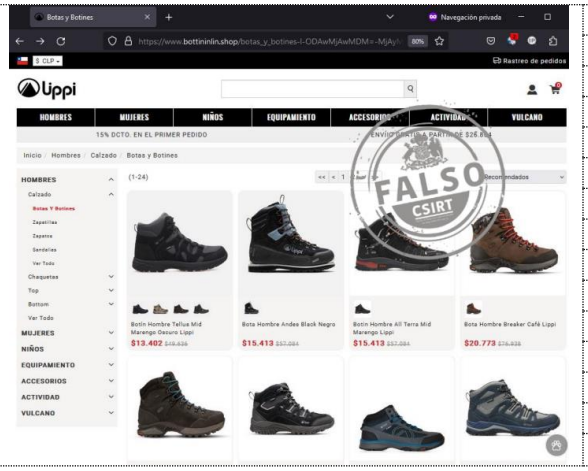
CSIRT alerta de nuevo sitio fraudulento que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR23-01427-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://juicydetox-q0zqt.line[.]pm/	
Dirección IP	
[162.248.224.250]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01427-01/	



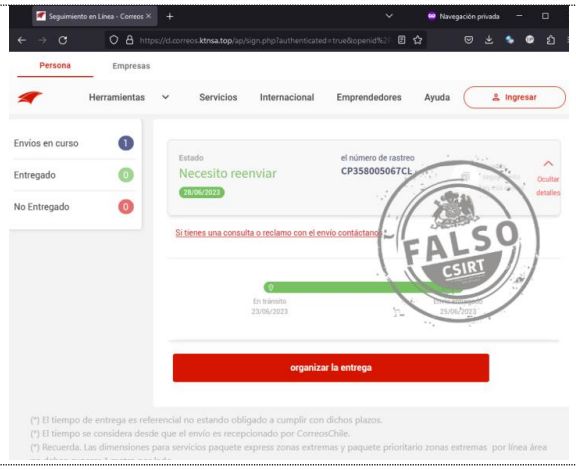
CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01428-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lippioutdoor-cl[.]shop/	
Dirección IP	
[104.21.38.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01428-01/	



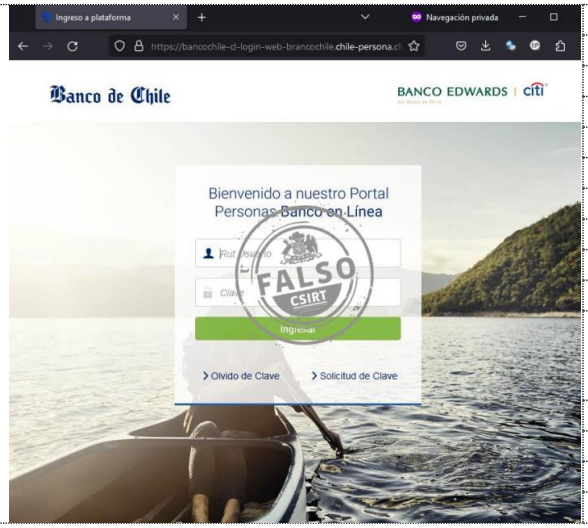
CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01429-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://santanderpersonas.my.canva[.]site/ https://www.kartaraharja.desa[.]id/santader/	
Dirección IP	
[103.147.154.46]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01429-01/	



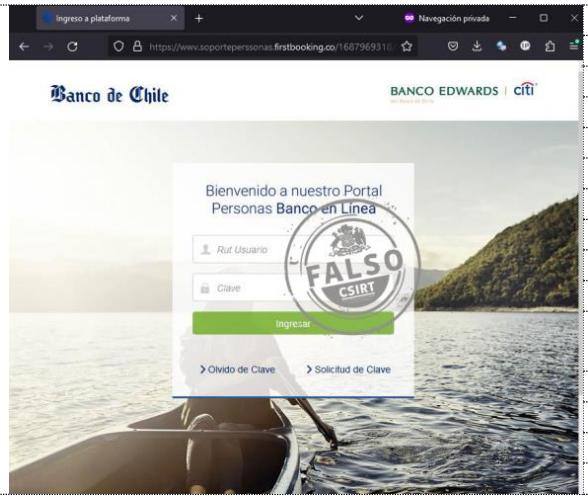
CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01430-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.bottininlin[.]shop	
Dirección IP	
[199.21.150.12]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01430-01/	



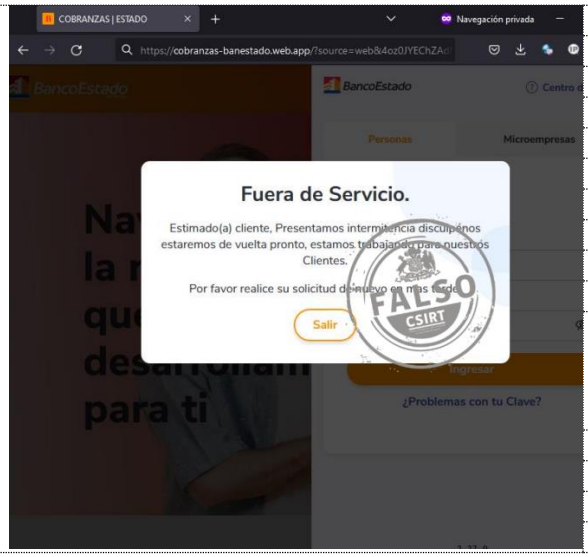
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01431-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://cl.correos.ktnsa[.]top	
Dirección IP	
[198.16.63.250]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01431-01/	



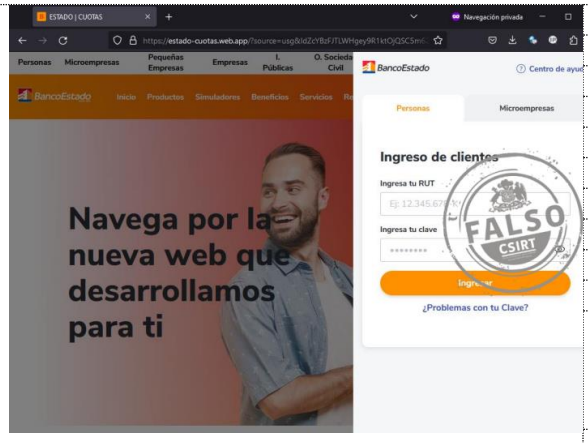
CSIRT alerta de un nuevo sitio fraudulento que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01432-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://tarjeta-cl[.]top/ https://bancochile-cl-login-web-brancochile.chile-persona[.]cfd/1687969063/bancochile-web/persona/login/index.html/login	
Dirección IP	
[172.67.172.105]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01432-01/	



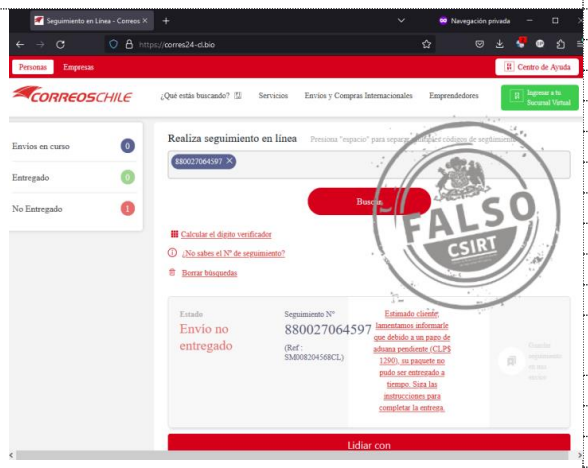
CSIRT alerta ante nueva página fraudulenta que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01433-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.soporteperssonas.firstbooking.co/1687969318/bchile-web/persona/login/index.html/login	
Dirección IP	
[85.187.142.74]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01433-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01434-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://bit[.]ly/40wP5AM http://134.209.150[.]51/2d8315d649d3fa31041dcde68f71b60b/f07298483f862fd852579faaefa696be?p=sofi https://cobranzas-banestado.web[.]app/?source=web	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01434-01/	

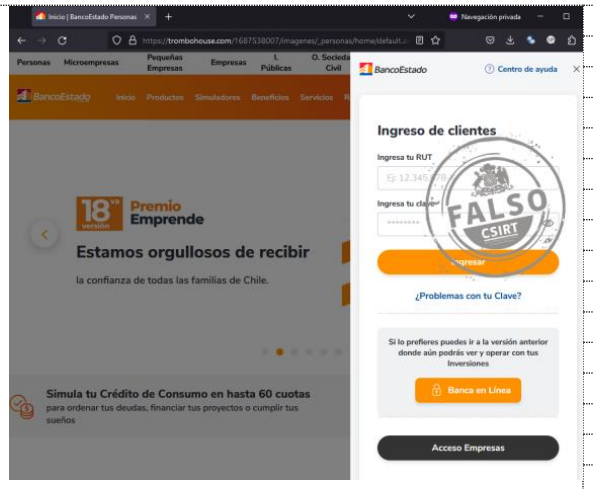


CSIRT alerta ante nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01435-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://bit[.]ly/3omdStp http://134.209.150[.]51/2d8315d649d3fa31041dcde68f71b60b/f07298483f862fd852579faaefa696be?p=indk https://estado-cuotas.web[.]app/?source=	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01435-01/	

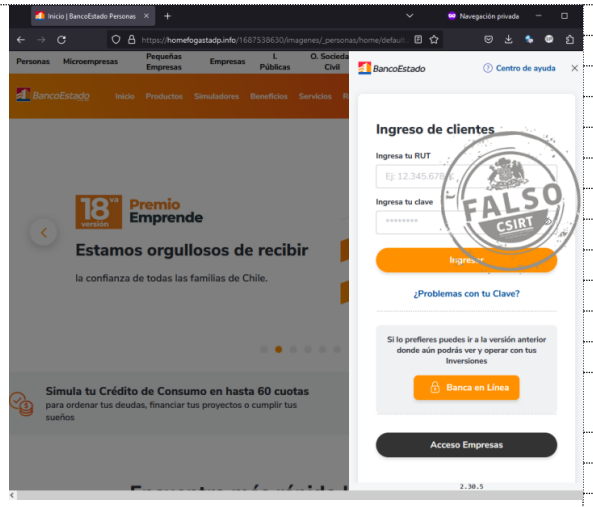


CSIRT alerta ante nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01436-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://s[.]id/1OcpY https://corres24-cl[.]bio/	
Dirección IP	
[64.176.5.56]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01436-01/	

2. Phishing

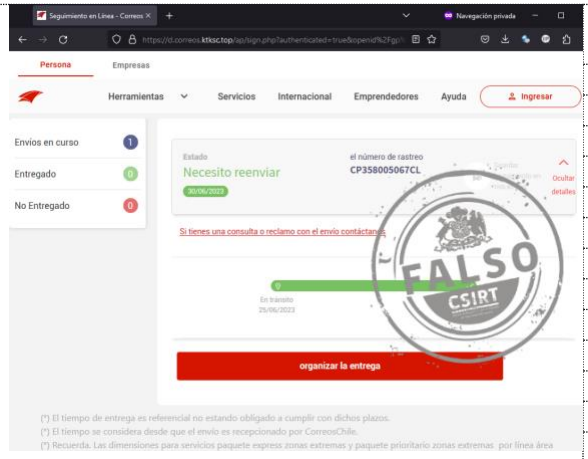


CSIRT alerta ante nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00839-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
URL redirección	
https://zoomcontactdoor[.]com/activacion/cuenta-dzqa/	
URL sitio falso	
https://trombohouse[.]com/1687538007/imagenes/_personas/home/default.asp	
Dirección IP	
[138.128.182.106]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00839-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00840-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de junio de 2023
Última revisión	27 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://proracingsimuladores[.]com.br/plugins/activacion/cuenta-ky/	
URL sitio falso	
https://homefogastadp[.]info/1687538630/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00840-01/	

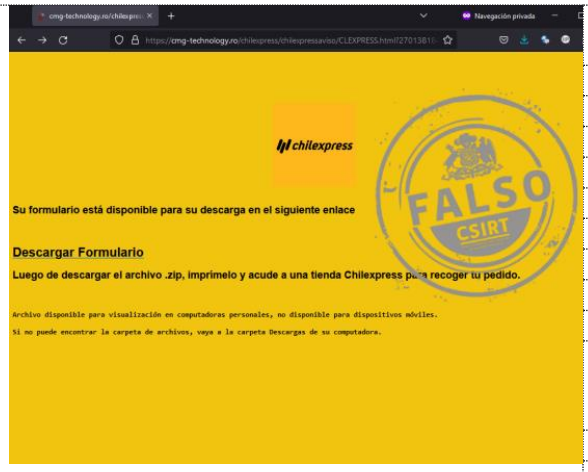
CSIRT alerta ante nueva página que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00842-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://is[.]gd/syw9id	
URL sitio falso	
https://cl-correos[.]top/#/?	
Dirección IP sitio falso	
[104.21.26.226]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00842-01/	



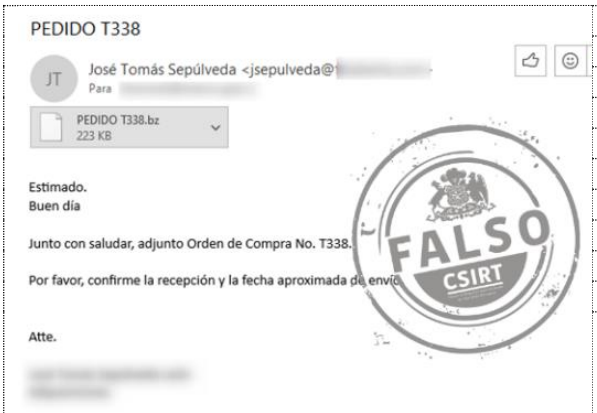
CSIRT alerta de nueva campaña de phishing via electrónico, que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00843-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://s[.]gd/CorReos	
URL sitio falso	
https://cl.correos.ktksc[.]top/ap/sign.php	
Dirección IP sitio falso	
[198.16.63.250]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00843-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing con malware en falso documento comercial	
Alerta de seguridad cibernética	2CMV23-00420-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
Indicadores de compromiso	
URL-Dominio	
40.79.189[.]59 209.197.3[.]8 http://api.ipify[.]org/	
SHA256	
4fd825574f5084d155dc6deacedb51ba422cc3904b651af71b7298a9e8ab202f 371de82ecda3f11d11e98a6265274bb708b2350ad47c77b4319da1d51764f64b	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00420-01/	



CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Chilexpress	
Alerta de seguridad cibernética	2CMV23-00421-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio de 2023
Indicadores de compromiso	
URL-Dominio	
https://cmg-technology[.]ro/chilexpress/chilexpressaviso/CLEXPRESS.html?270138184 https://nabaacademy[.]com/vendor/chilexpress/	
SHA256	
1fc3c3ad207309eede611ccafe91035b75163fd1fcf37db6fc61a6b251bcfe78 c3dd7c57ce52dd98cdac96e7bbb3c9b99fe55f1b62989f793ad8eb68d29c1e70 d8c9ea8a886e7e97048aaddb113f3220ed47535942cc3951316cab1a9489605e 07341bf5f2e5b9bf5cc9179a9a93b6eaee4417f92498d348933ea09e0742e055	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00421-01/	



CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Falabella	
Alerta de seguridad cibernética	2CMV23-00422-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2023
Última revisión	29 de junio de 2023
Indicadores de compromiso	
URL-Dominio	
www.gudusisamfbank[.]africa/a04y/ 154.64.247[.]44 64.190.63[.]111 64.190.62[.]22	
SHA256	
653025b16f9404285563b3e17df27b665689d0e8d85a021c90e111ad07c96136 3a338ce32d49e5b279311019e01551483c6a90c0d013be2336a65bb2fd15b10b ea474ba40224d8899c19d1dacf9fb88d39ab65eba3cbddb0fa41c4da05c5b663	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00422-01/	

4. Vulnerabilidades

CSIRT comparte información de vulnerabilidades parchadas para varios productos Apple	
Alerta de seguridad cibernética	9VSA23-00853-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 junio, 2023
Última revisión	23 junio, 2023
CVE	
CVE-2023-32434 CVE-2023-32435	CVE-2023-32439
Fabricante	
Apple	
Productos afectados	
iPhone 6s, iPhone 7, iPhone SE (1ra gen.), iPad Air 2, iPad mini (4ta gen.), and iPod touch (7ma gen.), iPhone 8 y posteriores, iPad Pro, iPad Air 3ra gen. y posteriores, iPad 5ta gen. y posteriores, iPad mini 5ta gen. y posteriores. macOS Big Sur. macOS Monterey. macOS Ventura. Apple Watch S4 y posteriores, Apple Watch S3, S4, S5, S6, S7, and SE.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00853-01/	

CSIRT comparte información de vulnerabilidades parchadas en FortiNAC de Fortinet, una crítica	
Alerta de seguridad cibernética	9VSA23-00854-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 junio, 2023
Última revisión	27 junio, 2023
CVE	
CVE-2023-33299	CVE-2023-33300
Fabricante	
Fortinet	
Productos afectados	
FortiNAC versiones 9.4.0 a9.4.2 FortiNAC versiones 9.2.0 a9.2.7 FortiNAC versiones 9.1.0 a9.1.9 FortiNAC versiones 7.2.0 a7.2.1 FortiNAC 8.8 todas las versiones FortiNAC 8.7 todas las versiones FortiNAC 8.6 todas las versiones FortiNAC 8.5 todas las versiones FortiNAC 8.3 todas las versiones	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00854-01/	

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.

- Rigoberto Cancino
- Carlos de la Fuente
- Juan Alberto Coppia Arena
- Alonso Ignacio Villalobos González
- Jair Palma
- Lucas Esteban Mardones Alvear
- Romel Rivas
- Francisco Esteban Solís Maturana
- Carlos David Escalona

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.30 16:09:09 -04'00'