CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 198

semana del 14 al 20 de abril de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

28 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

237 Las mitigaciones son útiles en productos de Oracle y Google (Chrome).

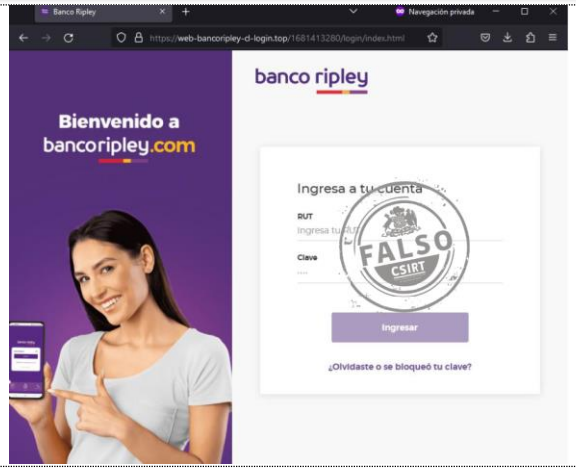
HASH REPORTADOS

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

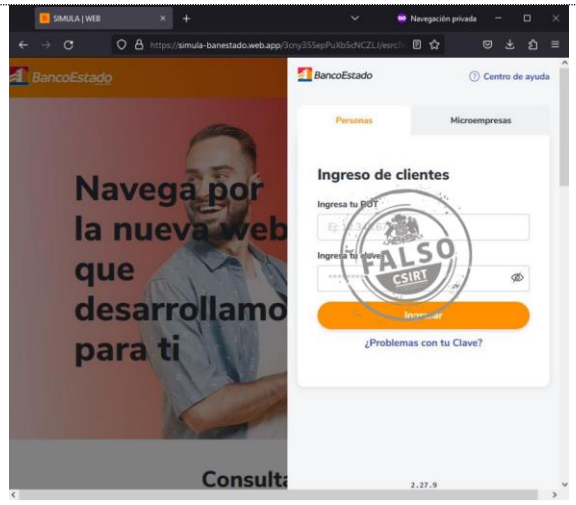
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

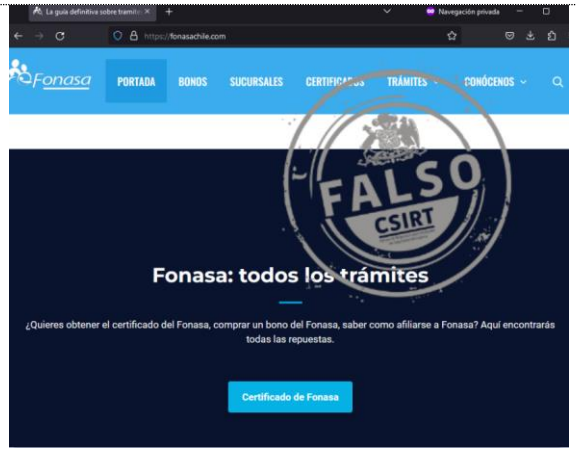


CSIRT alerta de página fraudulenta que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01280-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web-bancoripley-cl-login[.]top/1681413280/login/index.html	
Dirección IP	
[172.64.80.1]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01280-01	

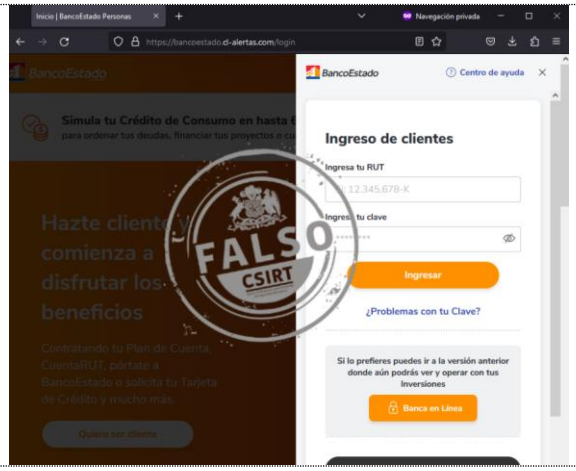


CSIRT alerta de página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01281-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//simula-banestado.web[.]app/3cny35SepPuXb5cNCZLJ/esrc?source=true&node=o7ehmh74qp1	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01281-01	

CSIRT alerta de página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01282-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//vv-oftor[.]xyz/es/4592-v2/?aff_sub=f7249usa4syzwd3c	
Dirección IP	
[104.21.2.56]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01282-01	



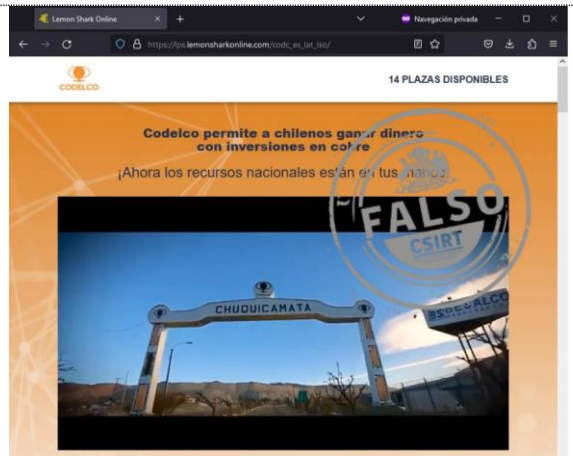
CSIRT alerta de sitio fraudulento que suplanta a Fonasa	
Alerta de seguridad cibernética	8FFR23-01283-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//fonasachile[.]com/	
Dirección IP	
[66.225.241.7]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01283-01	



CSIRT alerta de web fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01284-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//bancoestado.cl-alertas[.]com/login	
Dirección IP	
[104.21.71.48]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01284-01	

CSIRT alerta de página web fraudulenta que suplanta a SQM	
Alerta de seguridad cibernética	8FFR23-01285-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//read-offers[.]com/empresario/	
Dirección IP	
[172.67.173.213]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01285-01	

CSIRT informa de nuevo sitio fraudulento que suplanta a CCU	
Alerta de seguridad cibernética	8FFR23-01286-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//read-offers.com/ccu-es	
Dirección IP	
[104.21.40.8]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01286-01	

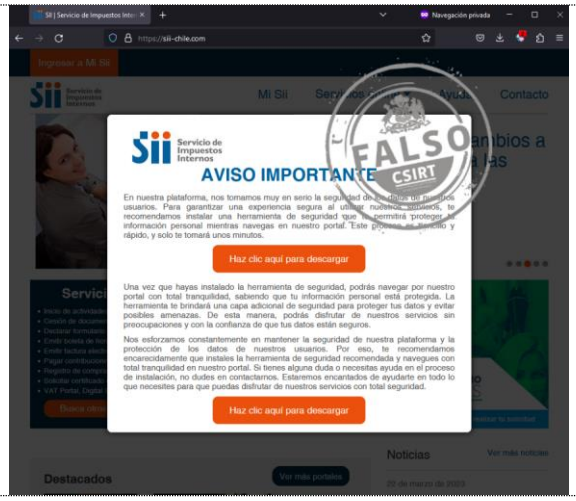


CSIRT alerta de nueva campaña de phishing que suplanta a Codelco	
Alerta de seguridad cibernética	8FFR23-01287-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril 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/8ffr23-01287-01	

CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01288-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2023
Última revisión	19 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//asistencia-banestado.web.app/GXREFGTA/ZDpQuJXJNnhL	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01288-01	

CSIRT alerta de página fraudulenta que suplanta a Banco Itaú	
Alerta de seguridad cibernética	8FFR23-01289-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2023
Última revisión	19 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//itau.impuestoschile[.]com/	
Dirección IP	
[20.226.87.125]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01289-01	

CSIRT alerta de sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01290-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//santander.impuestoschile[.]com/ santandrimpuestoscl[.]com	
Dirección IP	
[20.226.87.125]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01290-01	

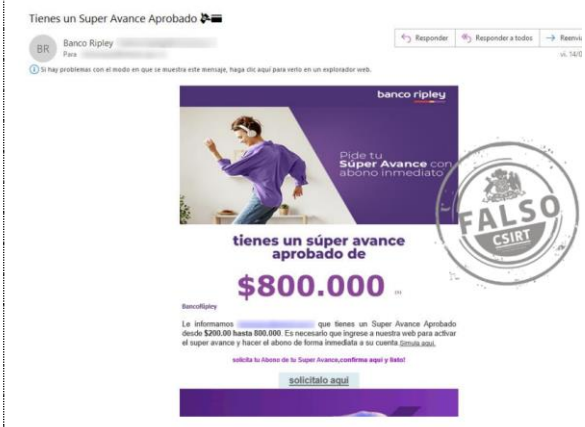


CSIRT alerta de sitio fraudulento que suplanta al SII	
Alerta de seguridad cibernética	8FFR23-01291-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
sii-home.supernovatextil[.]com.mx https[:]//siii-chile.com/	
Dirección IP	
[185.193.127.67]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01291-01	

CSIRT advierte ante nueva página fraudulenta que suplanta a SQM	
Alerta de seguridad cibernética	8FFR23-01292-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//real-invest-offer.com/es?campaign_id=sGMNdnt8&c=wlkbv906vcn0m65oistvf1cm&p1=mpandawh&p4=sqm&theme=ccu&ksget=1&analytics_session_id=822153736ca2839f78ce010652c61018582913ec1682001540&token=64414e84b6f54480b60ac658	
Dirección IP	
[172.67.173.59]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01292-01	

2. Phishing

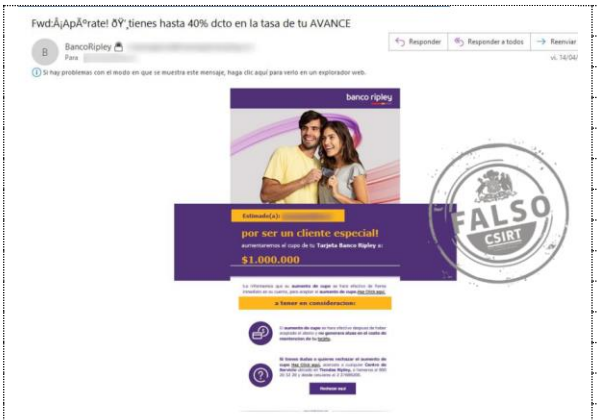
CSIRT alerta de nueva campaña de phishing via correo electrónico, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00786-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
URL redirección	
https[:]//clubmenthalist[.]com/promocion/cuenta-ooqn/	
URL sitio falso	
https[:]//nwmmayorsa[.]com/1681477326/imagenes/_personas/home/default.asp	
Dirección IP	
[67.23.242.202]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00786-01/	



CSIRT alerta de nueva campaña de phishing, que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00787-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web-bancoripley-cl.web-bancoripley-cl-login[.]info/1681477859/login/index.html	
URL redirección:	
https://aumento-portal[.]top/	
Dirección IP sitio falso	
[104.21.5.185]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00787-01/	

CSIRT alerta de nueva campaña de phishing por correo electrónico, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00788-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//estadofogapecl[.]top/1681479030/imagenes/_personas/home/default.asp	
URL redirección:	
https[:]//www.ideaprisma[.]it/online/activacion/cuenta-kzho/	
Dirección IP sitio falso	
[104.21.81.49]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00788-01/	

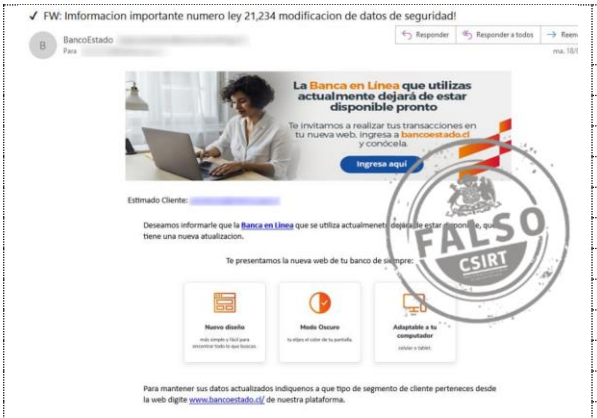
CSIRT alerta de nueva campaña de phishing que suplanta a Itaú Empresas	
Alerta de seguridad cibernética	8FPH23-00789-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL redirección:	
https[:]//www.wingedpeople.net/Photo/–/ https[:]/banco.itau.cl/?cliente=test@csirt.gob.cl	
URL sitio falso:	
https[:]//itau.sii-impuestoscl[.]com/	
Dirección IP sitio falso	
[20.226.87.125]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00789-01/	



CSIRT alerta de nueva campaña de phishing, que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00790-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//bit[.]ly/3KWZi4k?l=www.bancoripley.cl	
URL sitio falso	
https[:]//web.bancoripley.cl.berleymate.co[.]nz/1681497760/login	
Dirección IP	
[185.184.154.1]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00790-01/	

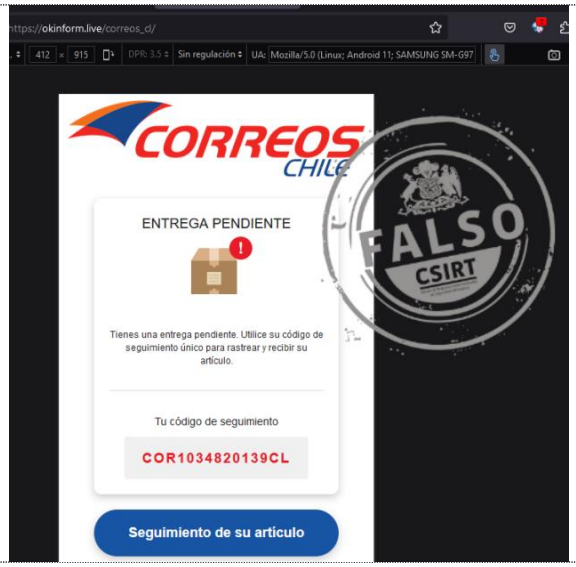
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00791-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2023
Última revisión	17 de abril de 2023
Indicadores de compromiso	
URL redirección	
https[:]//www.ideaprisma[.]it/online/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//estadofogapecl[.]top/1681744709/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.81.49]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00791-01/	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00792-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2023
Última revisión	18 de abril de 2023
Indicadores de compromiso	
URL redirección	
https[:]//clubmenthalist[.]com/promocion/cuenta-ooqn/	
URL sitio falso	
https[:]//nwmmayorsa[.]com/1681745339/imagenes/_personas/home/default.asp	
Dirección IP	
[67.23.242.202]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00792-01/	

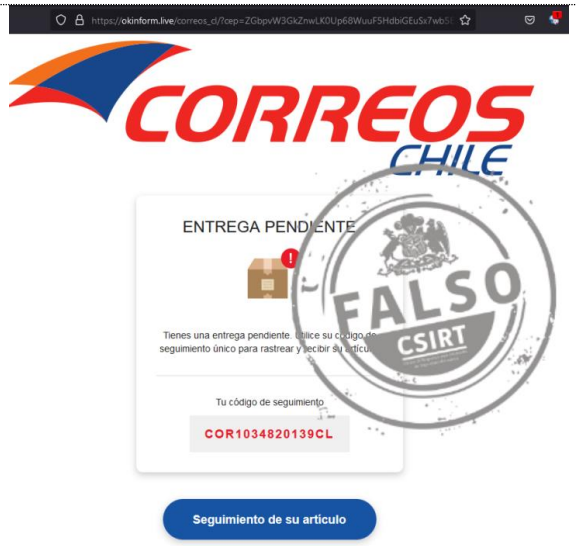


CSIRT informa de nueva campaña de phishing via email, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00793-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2023
Última revisión	18 de abril de 2023
Indicadores de compromiso	
URL redirección	
https[:]//www.ideaprisma[.]it/online/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//smshomefogapestados[.]top/1681833044/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.22.94]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00793-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00794-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2023
Última revisión	19 de abril de 2023
Indicadores de compromiso	
URL redirección	
https[:]//www.ideaprisma[.]it/online/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//smshomefogapestados[.]top/1681920505/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.22.94]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00794-01/	



CSIRT alerta de campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00795-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
Indicadores de compromiso	
URL redirección	
http[:]//jlhq.me/Zs0OIS	
URL sitio falso	
https[:]//okinform.live/correos_cl/ https[:]//www.online-giveaway-club.online/?gra=ee65854	
Dirección IP	
[185.112.146.238]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00795-01/	



CSIRT alerta de campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00796-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
Indicadores de compromiso	
URL redirección	
http[:]//hgxd.me/Zs0IKz	
URL sitio falso	
https[:]//okinform.live/correos_cl/ https[:]//www.online-giveaway-club.online/?gra=ee65854	
Dirección IP	
[185.112.146.238]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00796-01/	

3. Vulnerabilidades

CSIRT comparte información de vulnerabilidad día cero parchada para Google Chrome	
Alerta de seguridad cibernética	9VSA23-00818-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2023
Última revisión	18 de abril de 2023
CVE	
CVE-2023-2033	
Fabricantes	
Google	
Productos afectados	
Google Chrome.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00818-01/	

CSIRT comparte vulnerabilidades parchadas por Oracle en su Critical Patch Update de Abril 2023		
Alerta de seguridad cibernética	9VSA23-00819-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 de abril de 2023	
Última revisión	10 de abril de 2023	
CVE		
CVE-2018-1000656	CVE-2022-29599	CVE-2023-21927
CVE-2018-1311	CVE-2022-31081	CVE-2023-21928
CVE-2018-14371	CVE-2022-31123	CVE-2023-21929
CVE-2019-10086	CVE-2022-31129	CVE-2023-21930
CVE-2019-11287	CVE-2022-31160	CVE-2023-21931
CVE-2019-12415	CVE-2022-31630	CVE-2023-21932
CVE-2019-18935	CVE-2022-31692	CVE-2023-21933
CVE-2019-20916	CVE-2022-3171	CVE-2023-21934
CVE-2020-11987	CVE-2022-32215	CVE-2023-21935
CVE-2020-11988	CVE-2022-33980	CVE-2023-21936
CVE-2020-13936	CVE-2022-34169	CVE-2023-21937
CVE-2020-13954	CVE-2022-34305	CVE-2023-21938
CVE-2020-14343	CVE-2022-3479	CVE-2023-21939
CVE-2020-15250	CVE-2022-35737	CVE-2023-21940
CVE-2020-17521	CVE-2022-36033	CVE-2023-21941
CVE-2020-25638	CVE-2022-36760	CVE-2023-21942
CVE-2020-25649	CVE-2022-37434	CVE-2023-21943
CVE-2020-28052	CVE-2022-37865	CVE-2023-21944
CVE-2020-35168	CVE-2022-38752	CVE-2023-21945
CVE-2020-35169	CVE-2022-39271	CVE-2023-21946
CVE-2020-36518	CVE-2022-40146	CVE-2023-21947
CVE-2020-6950	CVE-2022-40149	CVE-2023-21948
CVE-2020-7009	CVE-2022-40151	CVE-2023-21952

	CVE-2020-7712	CVE-2022-40152	CVE-2023-21953
	CVE-2020-8908	CVE-2022-40304	CVE-2023-21954
	CVE-2021-22569	CVE-2022-41881	CVE-2023-21955
	CVE-2021-23017	CVE-2022-41966	CVE-2023-21956
	CVE-2021-23413	CVE-2022-42003	CVE-2023-21959
	CVE-2021-2351	CVE-2022-42004	CVE-2023-21960
	CVE-2021-23926	CVE-2022-42252	CVE-2023-21962
	CVE-2021-27568	CVE-2022-42889	CVE-2023-21963
	CVE-2021-29425	CVE-2022-42890	CVE-2023-21964
	CVE-2021-30129	CVE-2022-42898	CVE-2023-21965
	CVE-2021-31684	CVE-2022-42916	CVE-2023-21966
	CVE-2021-34798	CVE-2022-43401	CVE-2023-21967
	CVE-2021-35043	CVE-2022-43402	CVE-2023-21968
	CVE-2021-36090	CVE-2022-43548	CVE-2023-21969
	CVE-2021-36373	CVE-2022-43551	CVE-2023-21970
	CVE-2021-36374	CVE-2022-43680	CVE-2023-21971
	CVE-2021-3712	CVE-2022-4415	CVE-2023-21972
	CVE-2021-37519	CVE-2022-45047	CVE-2023-21973
	CVE-2021-37533	CVE-2022-45061	CVE-2023-21976
	CVE-2021-37695	CVE-2022-45143	CVE-2023-21977
	CVE-2021-4048	CVE-2022-45685	CVE-2023-21978
	CVE-2021-40690	CVE-2022-45693	CVE-2023-21979
	CVE-2021-41183	CVE-2022-46364	CVE-2023-21980
	CVE-2021-41184	CVE-2022-46908	CVE-2023-21981
	CVE-2021-41973	CVE-2022-47629	CVE-2023-21982
	CVE-2021-42575	CVE-2023-0215	CVE-2023-21984
	CVE-2021-43859	CVE-2023-0361	CVE-2023-21985
	CVE-2021-44832	CVE-2023-0662	CVE-2023-21986
	CVE-2021-46848	CVE-2023-1370	CVE-2023-21987
	CVE-2022-1292	CVE-2023-21896	CVE-2023-21988
	CVE-2022-1471	CVE-2023-21902	CVE-2023-21989
	CVE-2022-1587	CVE-2023-21903	CVE-2023-21990
	CVE-2022-2048	CVE-2023-21904	CVE-2023-21991
	CVE-2022-21824	CVE-2023-21905	CVE-2023-21992
	CVE-2022-2274	CVE-2023-21906	CVE-2023-21993
	CVE-2022-22965	CVE-2023-21907	CVE-2023-21996
	CVE-2022-22971	CVE-2023-21908	CVE-2023-21997
	CVE-2022-22978	CVE-2023-21909	CVE-2023-21998
	CVE-2022-22979	CVE-2023-21910	CVE-2023-21999
	CVE-2022-23181	CVE-2023-21911	CVE-2023-22000
	CVE-2022-23305	CVE-2023-21912	CVE-2023-22001
	CVE-2022-23437	CVE-2023-21913	CVE-2023-22002
	CVE-2022-23457	CVE-2023-21915	CVE-2023-22003
	CVE-2022-23491	CVE-2023-21916	CVE-2023-22899
	CVE-2022-24729	CVE-2023-21917	CVE-2023-23914
	CVE-2022-24839	CVE-2023-21918	CVE-2023-23916
	CVE-2022-25315	CVE-2023-21919	CVE-2023-23931
	CVE-2022-25647	CVE-2023-21920	CVE-2023-24998
	CVE-2022-25857	CVE-2023-21921	CVE-2023-25136
	CVE-2022-27404	CVE-2023-21922	CVE-2023-25194
	CVE-2022-28199	CVE-2023-21923	CVE-2023-25577
	CVE-2022-28327	CVE-2023-21924	CVE-2023-25613
	CVE-2022-28738	CVE-2023-2192	CVE-2023-25690
	CVE-2022-29577	CVE-2023-21926	CVE-2023-28708

Fabricantes
Oracle
Productos afectados
JD Edwards EnterpriseOne Orchestrator
JD Edwards EnterpriseOne Tools
JD Edwards World Security
Management Cloud Engine
Oracle Access Manager
Oracle Agile PLM
Oracle Application Object Library
Oracle Application Testing Suite
Oracle Argus Insight
Oracle Argus Safety
Oracle Banking APIs
Oracle Banking Corporate Lending
Oracle Banking Corporate Lending Process Management
Oracle Banking Digital Experience
Oracle Banking Payments
Oracle Banking Trade Finance
Oracle Banking Treasury Management
Oracle Banking Virtual Account Management
Oracle BI Publisher
Oracle Blockchain Platform
Oracle Business Intelligence Enterprise Edition
Oracle Business Process Management Suite
Oracle Clinical Remote Data Capture
Oracle Coherence
Oracle Commerce Guided Search
Oracle Commerce Platform
Oracle Communications Cloud Native Configuration Console
Oracle Communications Cloud Native Core Automated Test Suite
Oracle Communications Cloud Native Core Binding Support Function
Oracle Communications Cloud Native Core Console
Oracle Communications Cloud Native Core Network Exposure Function
Oracle Communications Cloud Native Core Network Function Cloud Native Environment
Oracle Communications Cloud Native Core Network Repository Function
Oracle Communications Cloud Native Core Policy
Oracle Communications Cloud Native Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy
Oracle Communications Cloud Native Core Unified Data Repository
Oracle Communications Convergent Charging Controller
Oracle Communications Core Session Manager
Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager
Oracle Communications IP Service Activator
Oracle Communications Network Charging and Control
Oracle Communications Operations Monitor
Oracle Communications Order and Service Management
Oracle Communications Policy Management
Oracle Communications Services Gatekeeper
Oracle Communications Session Border Controller
Oracle Communications Session Report Manager
Oracle Communications Session Router
Oracle Communications Subscriber-Aware Load Balancer

	Oracle Communications Unified Assurance Oracle Communications Unified Inventory Management Oracle Communications User Data Repository Oracle Data Integrator Oracle Database OML4PY (Python) Oracle Database Recovery Manager Oracle Database Workload Manager (Apache Commons FileUpload) Oracle Documaker Oracle Enterprise Communications Broker Oracle Enterprise Manager Ops Center Oracle Enterprise Session Router Oracle Essbase Oracle Financial Services Analytical Applications Infrastructure Oracle Financial Services Analytical Applications Reconciliation Framework Oracle Financial Services Asset Liability Management Oracle Financial Services Balance Computation Engine Oracle Financial Services Balance Sheet Planning Oracle Financial Services Behavior Detection Platform Oracle Financial Services Compliance Studio Oracle Financial Services Crime and Compliance Management Studio Oracle Financial Services Currency Transaction Reporting Oracle Financial Services Data Governance for US Regulatory Reporting Oracle Financial Services Data Integration Hub Oracle Financial Services Deposit Insurance Calculations for Liquidity Risk Management Oracle Financial Services Enterprise Case Management Oracle Financial Services Enterprise Financial Performance Analytics Oracle Financial Services Funds Transfer Pricing Oracle Financial Services Institutional Performance Analytics Oracle Financial Services Liquidity Risk Measurement and Management Oracle Financial Services Loan Loss Forecasting and Provisioning Oracle Financial Services Model Management and Governance Oracle Financial Services Profitability Management Oracle Financial Services Regulatory Reporting Oracle Financial Services Regulatory Reporting with AgileREPORTER Oracle Financial Services Retail Performance Analytics Oracle Financial Services Revenue Management and Billing Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition Oracle FLEXCUBE Core Banking Oracle FLEXCUBE Universal Banking Oracle GoldenGate Oracle GoldenGate Studio Oracle GraalVM Enterprise Edition Oracle Graph Server and Client Oracle Health Sciences InForm Oracle Healthcare Foundation Oracle Healthcare Master Person Index Oracle Healthcare Translational Research Oracle Hospitality OPERA 5 Property Services Oracle HTTP Server Oracle Hyperion Financial Reporting Oracle Hyperion Infrastructure Technology Oracle Identity Manager Oracle iLearning

	Oracle Insurance Policy Administration Operational Data Store for Life and Annuity Oracle iProcurement Oracle iReceivables Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle JDeveloper Oracle Managed File Transfer Oracle Middleware Common Libraries and Tools Oracle NoSQL Database Oracle Outside In Technology Oracle REST Data Services Oracle Retail Customer Management and Segmentation Foundation Oracle Retail Fiscal Management Oracle Retail Invoice Matching Oracle Retail Merchandising System Oracle Retail Predictive Application Server Oracle Retail Price Management Oracle Retail Sales Audit Oracle Retail Xstore Office Cloud Service Oracle Retail Xstore Point of Service Oracle SD-WAN Aware Oracle SD-WAN Edge Oracle SOA Suite Oracle Solaris Oracle SQL Developer Oracle User Management Oracle Utilities Application Framework Oracle Utilities Network Management System Oracle VM VirtualBox Oracle WebCenter Portal Oracle WebCenter Sites Oracle WebLogic Server PeopleSoft Enterprise HCM Human Resources PeopleSoft Enterprise PeopleTools Primavera P6 Enterprise Project Portfolio Management Primavera Unifier Product Siebel CRM Spatial and Graph (Apache Commons Fileupload)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00819-01/

CSIRT comparte información de vulnerabilidades parchadas en Google Chrome, incluyendo una de día cero	
Alerta de seguridad cibernética	9VSA23-00820-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2023
Última revisión	20 de abril de 2023
CVE	
CVE-2023-2133	
CVE-2023-2134	
CVE-2023-2135	
CVE-2023-2136	
CVE-2023-2137	
Fabricantes	
Google	
Productos afectados	
Google Chrome	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00820-01/	

4. Malware

CSIRT alerta de nueva campaña de phishing con malware, con excusa de falsa notificación de deuda	
Alerta de seguridad cibernética	2CMV23-00409-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2023
Última revisión	14 de abril de 2023
Indicadores de compromiso	
URL-Dominio	
https[:]//drive.google[.]com/uc?id=1cC8ZfcW5tnx4fkeim9vZqE4kTuqgolJC&export=download&authuser=0 https[:]//pastebin[.]com/raw/fNYFJXVy https[:]//paste[.]ee/d/Leoqz/0	
SHA256	
6386a5b2fc971811f017788e2ea494dd02d5081bbf5e16624f8570f3fcc255c0 f0c8e37cc8ac1b6a035cf180f8f892a16bc1afa59a8edd33e53263e73be2dc5d b1860633c96be2e60353cf76801c6ea53df1761af69383337b297487748a044b	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00409-01/	

CSIRT alerta de campaña de phishing con malware, difundida en email con falsa notificación judicial	
Alerta de seguridad cibernética	2CMV23-00410-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2023
Última revisión	18 de abril de 2023
Indicadores de compromiso	
URL-Dominio	
datosinfomativos12.duckdns[.]org	
SHA256	
962a5fca2c50aa8bc385430470a2dbcea4178bccd2db7bfc90236deb415671b3 cfce37e21ebb8cf616e28184f63e02caf1ce5089b1bc875634582a10132e3ad2 c3896f1e64b642496218a979b1c5d48d77b9babd365a3d9cfd60a75e808a5b3d a7aad8d4e18a174e9efbec8e2658c62a6838f905832fc442f10427db857ed20e	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00410-01/	

5. Concientización

Ciberdiccionario Volumen 33

Nuevos términos para el Ciberdiccionario del CSIRT de Gobierno esta semana: eSIM, cadena de custodia, ataques man-in-the-middle y canal seguro. Como siempre, está disponible también en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-33/.

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.

- Mitchell Alarcon A.
- Carlos Ramirez
- Wilson Irribarra I.
- Rigoberto Cancino
- Marcelo Gutierrez E.
- Hellis Leiva
- Gonzalo Salazar

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.21 17:43:36 -04'00'