CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 209

semana del 30 de junio al 6 de julio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

628

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

32

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

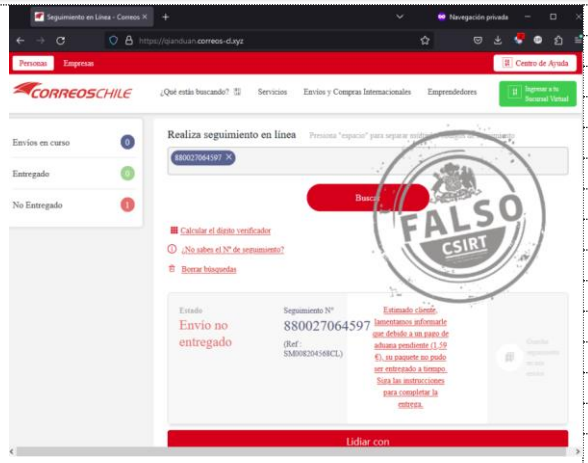
57

Las mitigaciones son útiles en productos de Google y Cisco.

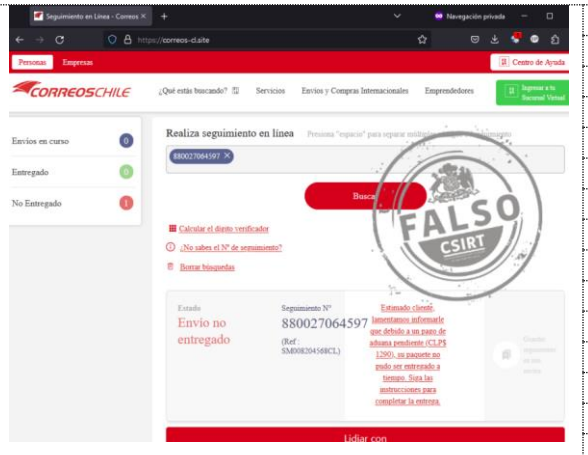
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

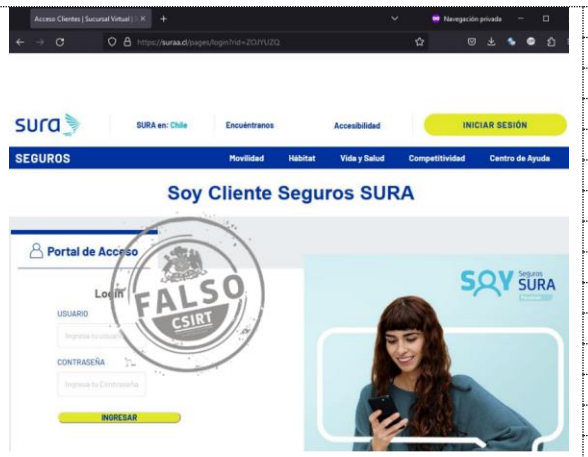
1. Sitios fraudulentos



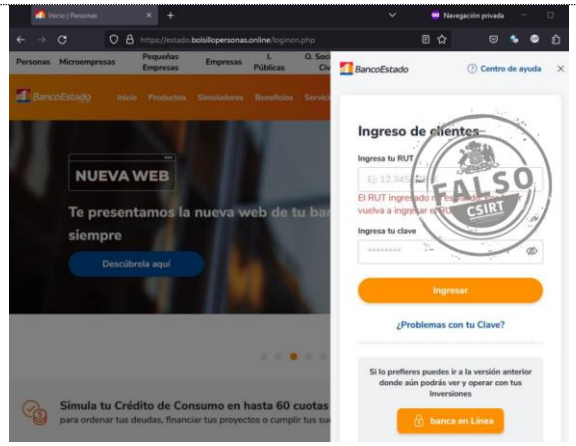
CSIRT alerta ante nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01437-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 junio, 2023
Última revisión	30 junio, 2023
Indicadores de compromiso	
URL sitio falso	
https://qianduan.correos-cl[.]xyz/	
Dirección IP	
[38.60.204.187]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01437-01/	



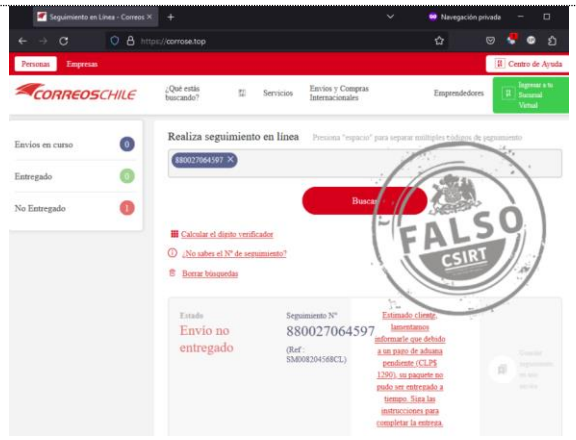
CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01438-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 junio, 2023
Última revisión	30 junio, 2023
Indicadores de compromiso	
URL sitio falso	
https://correos-cl[.]site/	
Dirección IP	
[45.15.160.151]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01438-01/	



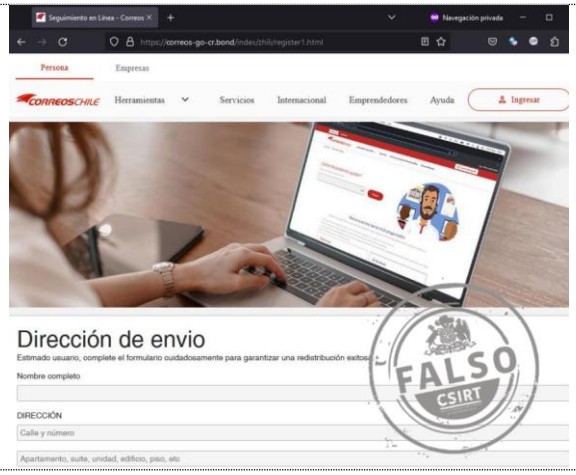
CSIRT alerta de nuevo sitio fraudulento que suplanta a Seguros Sura	
Alerta de seguridad cibernética	8FFR23-01439-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 junio, 2023
Última revisión	30 junio, 2023
Indicadores de compromiso	
URL sitio falso	
https://suraa[.]cl/pages/login?rid=ZOJYUZQ	
Dirección IP	
[165.232.159.114]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01439-01/	



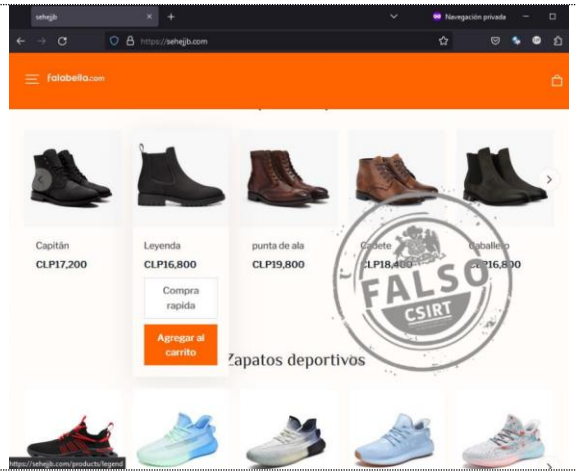
CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01440-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 julio, 2023
Última revisión	3 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://estado.bolsillopersonas[.[online/loginon.php	
Dirección IP	
[104.21.30.214]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01440-01/	



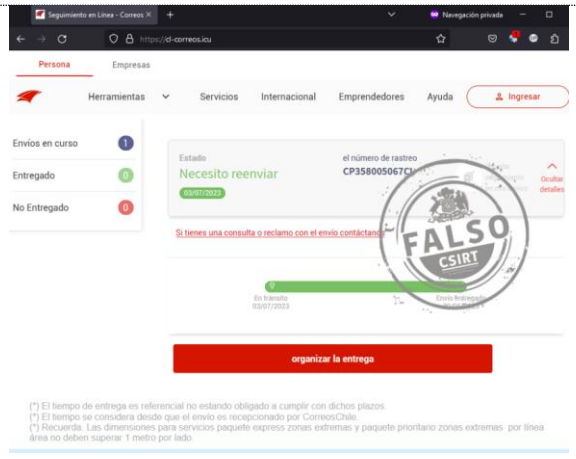
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01441-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://corrose[.]top/	
Dirección IP	
[170.106.106.43]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01441-01/	



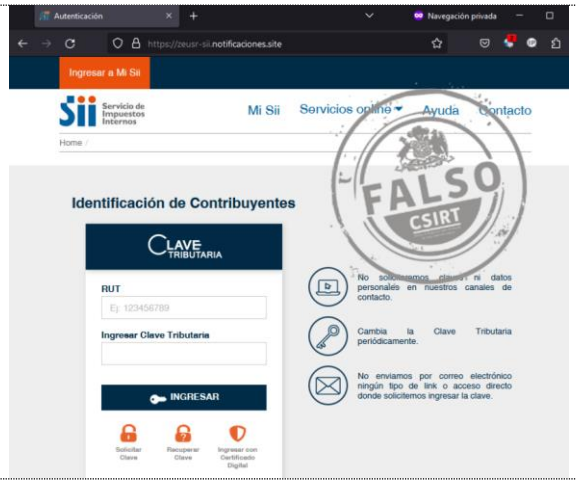
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01442-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://correos-go-cr[.]bond	
Dirección IP	
[172.67.160.206]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01442-01/	



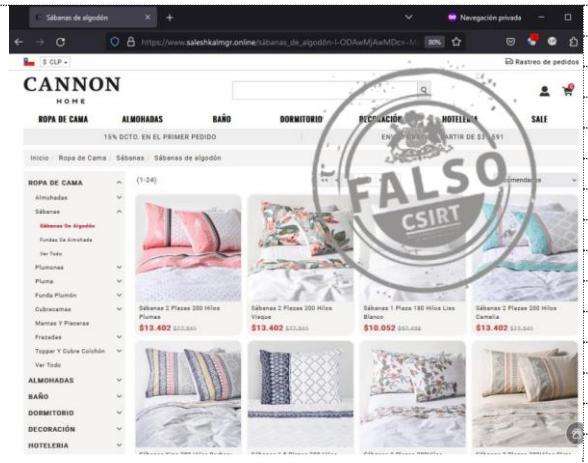
CSIRT alerta de nuevo sitio fraudulento que suplanta a Falabella.com	
Alerta de seguridad cibernética	8FFR23-01443-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://sehejjb[.]com/	
Dirección IP	
[104.17.232.29]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01443-01/	



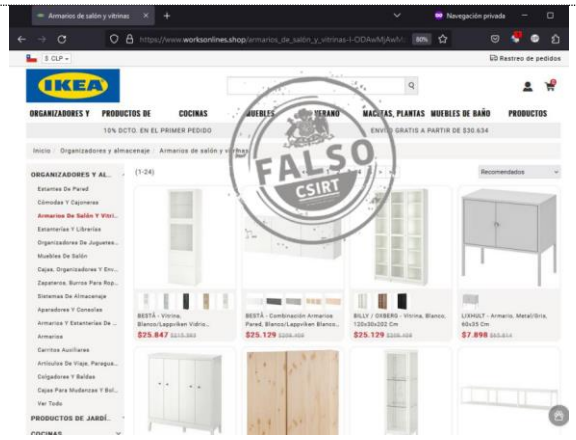
CSIRT alerta ante nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01444-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://cl-correos[.]icu/	
Dirección IP	
[155.94.179.81]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01444-01/	



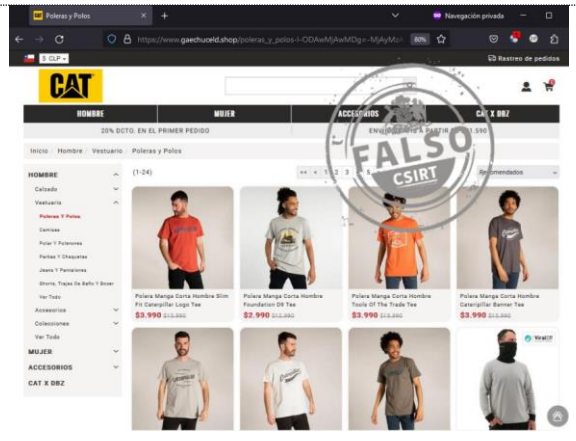
CSIRT alerta de sitio fraudulento que suplanta al Servicio de Impuestos Internos	
Alerta de seguridad cibernética	8FFR23-01445-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://zeusr-sii.notificaciones[.]site/	
Dirección IP	
[104.21.91.80]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01445-01/	



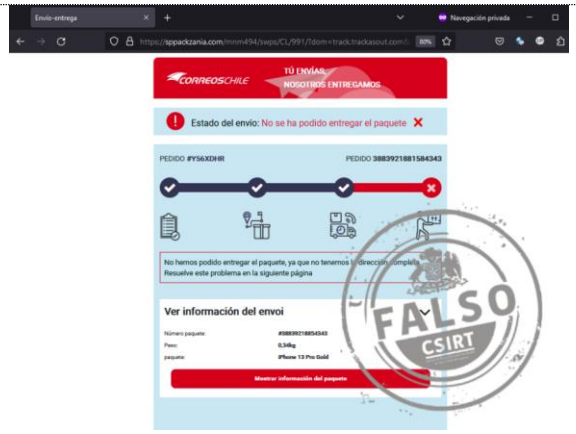
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cannon	
Alerta de seguridad cibernética	8FFR23-01446-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.saleshkalmgr[.]onlline	
Dirección IP	
[23.252.68.235]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01446-01/	



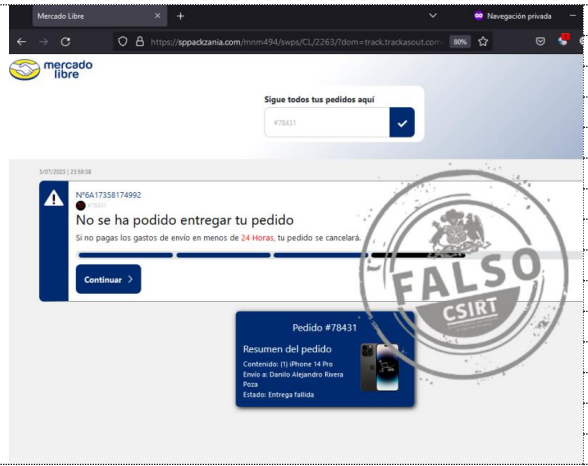
CSIRT alerta ante nuevo sitio fraudulento que suplanta a IKEA	
Alerta de seguridad cibernética	8FFR23-01447-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.worksonlines[.]shop	
Dirección IP	
[167.160.3.28]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01447-01/	



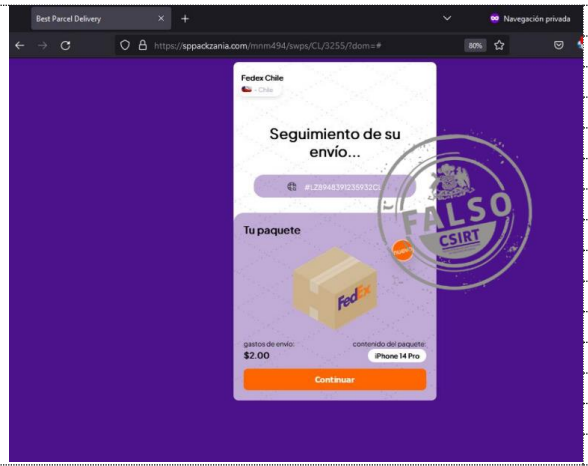
CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01448-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.gaechuceld[.]shop/	
Dirección IP	
[199.21.150.22]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01448-01/	



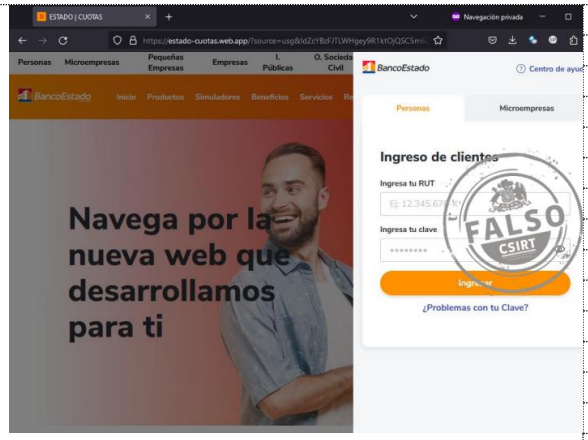
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01449-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://sppackzania[.]com	
Dirección IP	
[198.54.116.53]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01449-01/	



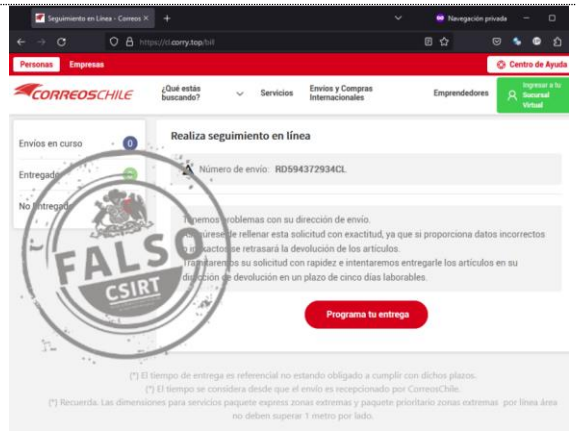
CSIRT alerta de nuevo sitio fraudulento que suplanta a Mercado Libre	
Alerta de seguridad cibernética	8FFR23-01450-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://sppackzania[.]com/mnm494/swps/CL/2263/?dom=#	
Dirección IP	
[198.54.116.53]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01450-01/	



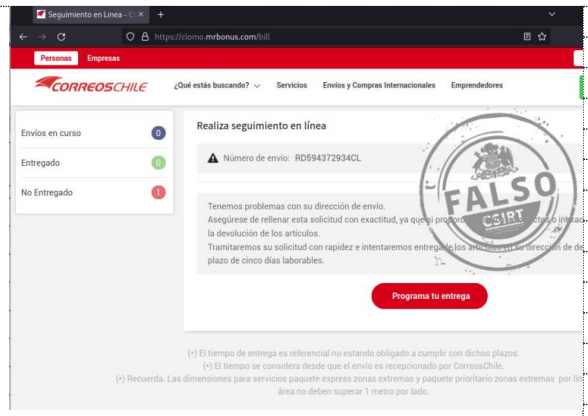
CSIRT alerta de nuevo sitio fraudulento que suplanta a FedEx	
Alerta de seguridad cibernética	8FFR23-01451-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://sppackzania[.]com/mnm494/swps/CL/3255/?dom=#	
Dirección IP	
[198.54.116.53]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01451-01/	



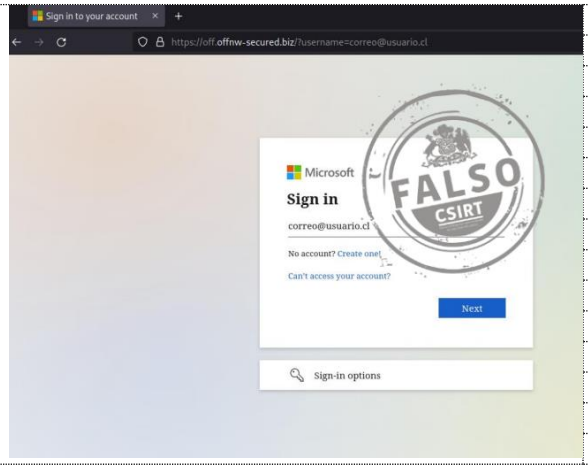
CSIRT alerta de nuevo sitio fraudulento que suplanta a Veja	
Alerta de seguridad cibernética	8FFR23-01452-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.vejachileoutlet[.]com/	
Dirección IP	
[165.231.154.228]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01452-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01453-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://cl.corry[.]top/bill	
Dirección IP	
[49.51.142.129]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01453-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01454-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://clomo.mrbonus[.]com/bill	
Dirección IP	
[49.51.142.129]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01454-01/	



CSIRT alerta ante sitio fraudulento que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR23-01455-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://off.offnw-secured[.]biz/?username=correo@usuario.cl	
Dirección IP	
[104.171.114.243]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01455-01/	

CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01456-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://ume[.]la/wsWsLB https://chl-poster-track[.]top/#/?	
Dirección IP	
[173.82.212.215]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01456-01/	

2. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta a Microsoft	
Alerta de seguridad cibernética	8FPH23-00844-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 julio, 2023
Última revisión	3 julio, 2023
URL sitio falso	
https://bafybeidi6jnktkimxnekniyoxskh6tddudimtadfyhvtn7ifyekais76em.ipfs.cf-ipfs.com/common/oauth2/?authoriseclient_id=4315ab9-913as3-40a0u-a4ut6-3536ade03&redirect_uri=https%3A%2F%2Fwww.office.com%2Flanding&response_type=code%20id_token&scope=openid%20profile&response_mode=form_post&nonce=637471761361998550.YTE5MmQzYzMtNTg2MS00NzQ4LTg5ZWQtOWQ3OGJiMjQ1MmE0MmUxOTg5NTQtYjFkOC00ZjhiLTlmMTUtMGE4ZTA0NWQyNzI2&ui_locales=en-US&mkt=en-US&client-request-id=68f9d7da-5456-46658e-88as69ads-06sad18ads19dsa076edb&state=Kck8msXjhXilh8v4_zjTdU2Y8mdE3_0__tttyi04kcOXzJoTHhQ1svBKB-jRrfgaTOJmXRCbtJ4MhyVHer_lbBxIQc1fngPy2KQ1PDy2bRhgW_B3CQiu4mC74gX2xXAL6ED040X0fitKWb16s7_lvfa_dHgwLhDdAj8YYTfOkJ-i_gR_Vwq9JV-PmXDli6FPm9jIY96qfojSHj9E_eYH4gsoIRDeKVRNQ456O12eZeHh8XklcKhwhMC0I5RWqoreJnf8ulumuhrlbzuxmIXBiQ&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=6.8.0.0	
Dirección IP	
[198.16.63.250]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00844-01/	

CSIRT alerta por una nueva campaña de phishing por email, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00845-01
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://reachercontact[.]com/activacion/cuenta-zksc/	
URL sitio falso	
https://fogapepatito[.]com/1688391038/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[138.128.188.146]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00845-01/	

CSIRT alerta de campaña de phishing a través de email extorsivo de carácter sexual	
Alerta de seguridad cibernética	8FPH23-00846-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 julio, 2023
Última revisión	4 julio, 2023

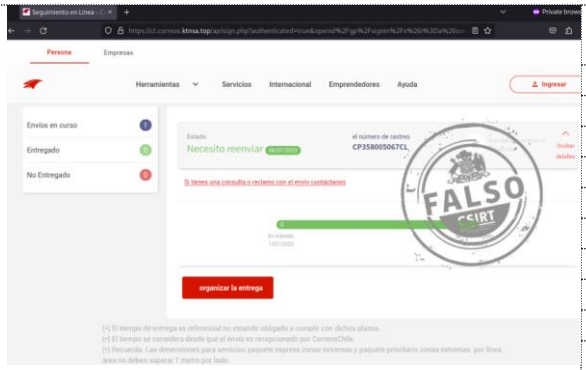
Indicadores de compromiso

Dirección IP sitio falso

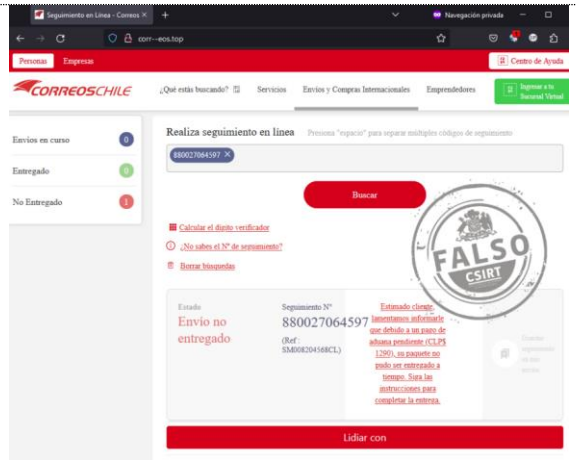
[1.244.45.204]	[154.125.225.243]	[187.73.25.252]	[39.118.249.66]
[101.53.216.118]	[154.125.47.238]	[187.85.87.15]	[39.121.84.213]
[102.132.132.220]	[154.236.124.254]	[187.87.25.118]	[39.32.165.238]
[102.141.54.105]	[154.240.227.115]	[188.112.100.57]	[39.33.230.151]
[102.142.102.49]	[154.56.136.29]	[188.126.200.27]	[39.36.151.105]
[102.156.12.127]	[154.70.30.13]	[188.164.147.94]	[39.36.197.103]
[102.156.180.17]	[154.72.153.66]	[188.251.55.79]	[39.37.35.63]
[102.158.185.223]	[154.72.171.146]	[188.37.251.116]	[39.40.124.203]
[102.164.196.45]	[160.120.203.60]	[188.70.45.165]	[39.41.244.22]
[102.173.216.164]	[160.154.233.27]	[188.71.220.56]	[39.43.243.9]
[102.216.201.33]	[160.176.141.120]	[189.111.251.124]	[39.43.48.115]
[102.217.178.10]	[160.178.27.233]	[189.124.0.84]	[39.53.172.25]
[102.64.221.106]	[160.179.3.255]	[189.202.86.241]	[39.55.141.66]
[102.65.63.224]	[161.230.60.188]	[189.4.95.56]	[39.62.2.230]
[102.67.1.71]	[164.127.236.180]	[190.102.68.76]	[41.115.109.125]
[102.68.77.227]	[164.160.93.205]	[190.106.118.205]	[41.116.184.5]
[102.78.24.158]	[165.73.133.116]	[190.108.85.50]	[41.129.104.142]
[103.101.111.233]	[167.0.223.235]	[190.111.97.182]	[41.129.116.238]
[103.106.239.60]	[167.179.38.62]	[190.115.102.209]	[41.141.246.8]
[103.121.121.234]	[167.56.202.246]	[190.129.165.78]	[41.141.59.102]
[103.124.207.53]	[167.56.98.109]	[190.135.177.236]	[41.142.30.139]
[103.138.250.135]	[167.62.116.210]	[190.154.136.18]	[41.142.57.235]
[103.145.108.133]	[168.167.26.235]	[190.17.18.143]	[41.158.189.92]
[103.147.8.72]	[168.181.96.180]	[190.17.247.55]	[41.175.105.156]
[103.153.127.35]	[168.194.136.186]	[190.186.64.120]	[41.191.78.163]
[103.154.156.10]	[168.194.15.183]	[190.20.238.189]	[41.198.138.96]
[103.165.68.119]	[168.90.12.165]	[190.210.32.253]	[41.215.219.84]
[103.167.232.209]	[170.231.133.37]	[190.211.179.237]	[41.216.201.18]
[103.167.75.49]	[170.233.32.156]	[190.235.208.52]	[41.216.202.172]
[103.170.161.2]	[170.233.78.161]	[190.239.126.166]	[41.250.179.22]
[103.174.168.44]	[170.79.54.26]	[190.239.165.96]	[41.85.163.203]
[103.190.41.47]	[170.82.50.190]	[191.178.74.121]	[41.90.68.121]
[103.20.55.5]	[170.83.132.144]	[191.185.78.60]	[41.90.70.136]
[103.204.68.25]	[171.224.177.241]	[191.191.65.125]	[43.252.15.255]
[103.212.158.205]	[171.233.43.171]	[191.243.229.24]	[43.254.126.6]
[103.216.68.109]	[171.236.129.10]	[191.246.225.110]	[45.164.102.218]
[103.216.71.154]	[171.236.65.67]	[191.37.243.221]	[45.165.251.98]
[103.249.251.46]	[171.237.139.78]	[191.53.77.216]	[45.166.249.155]
[103.3.220.83]	[171.238.79.154]	[191.95.138.159]	[45.166.85.131]
[103.3.221.64]	[171.246.162.193]	[191.95.175.95]	[45.167.205.134]
[103.3.81.21]	[171.252.153.61]	[191.97.78.133]	[45.170.130.152]
[103.38.38.130]	[171.61.154.154]	[192.141.147.106]	[45.171.175.135]
[103.39.10.112]	[172.117.49.40]	[193.187.102.229]	[45.178.193.176]
[103.39.51.82]	[175.100.20.230]	[196.188.162.52]	[45.180.191.29]
[103.41.95.24]	[175.176.55.3]	[196.188.193.47]	[45.181.123.4]
[103.42.91.50]	[175.176.65.213]	[196.189.242.32]	[45.183.18.0]
[103.47.33.252]	[175.176.7.156]	[196.190.60.189]	[45.184.172.2]
[103.48.183.101]	[175.209.80.242]	[196.191.116.129]	[45.188.27.109]
[103.49.115.206]	[176.151.86.89]	[196.200.235.147]	[45.226.98.17]
[103.49.255.109]	[176.236.21.99]	[196.201.246.253]	[45.232.34.55]

	[103.62.152.242]	[176.63.4.232]	[196.203.239.223]	[45.237.44.165]
	[103.83.235.162]	[177.101.168.74]	[196.217.70.74]	[45.238.122.68]
	[103.85.112.2]	[177.12.180.225]	[196.234.231.119]	[45.238.243.231]
	[105.112.249.10]	[177.124.1.67]	[196.251.243.10]	[45.241.177.101]
	[105.113.12.225]	[177.128.190.199]	[196.64.219.156]	[45.244.131.242]
	[105.154.216.237]	[177.129.145.17]	[196.64.220.51]	[45.247.24.121]
	[105.155.240.71]	[177.140.105.196]	[196.65.26.81]	[45.247.44.32]
	[105.156.124.45]	[177.152.157.56]	[196.89.175.160]	[45.250.158.183]
	[105.156.134.108]	[177.154.4.152]	[197.1.170.85]	[45.4.62.240]
	[105.158.109.69]	[177.185.40.239]	[197.10.121.29]	[45.7.212.158]
	[105.160.54.77]	[177.235.129.88]	[197.113.95.117]	[45.71.81.239]
	[105.224.34.169]	[177.235.63.10]	[197.118.37.5]	[46.114.38.83]
	[105.224.52.139]	[177.36.176.125]	[197.15.70.129]	[46.217.78.84]
	[105.235.131.29]	[177.36.201.115]	[197.167.187.33]	[46.225.209.201]
	[106.104.102.242]	[177.38.189.96]	[197.219.107.22]	[46.99.1.254]
	[106.207.16.89]	[177.43.63.97]	[197.237.123.21]	[49.0.66.41]
	[109.196.114.20]	[177.50.201.246]	[197.237.130.183]	[49.215.22.57]
	[109.205.139.237]	[177.72.109.187]	[197.237.244.3]	[49.228.125.167]
	[109.228.210.14]	[177.74.142.67]	[197.240.109.112]	[49.228.61.156]
	[109.43.51.175]	[177.8.227.184]	[197.26.197.176]	[49.43.249.117]
	[110.39.174.69]	[177.87.253.254]	[197.3.251.134]	[5.146.193.167]
	[111.119.187.0]	[177.89.194.1]	[198.72.227.15]	[5.172.238.142]
	[112.148.80.176]	[178.175.109.98]	[199.223.250.219]	[5.173.198.44]
	[112.150.154.6]	[178.235.186.203]	[2.206.211.49]	[5.173.206.16]
	[112.197.45.177]	[178.244.198.52]	[2.38.229.11]	[5.214.177.115]
	[112.215.172.132]	[178.25.144.16]	[2.39.114.118]	[5.249.75.104]
	[113.162.50.177]	[178.51.89.200]	[2.39.23.252]	[5.62.145.22]
	[113.173.182.178]	[178.75.238.194]	[200.102.96.187]	[5.91.61.113]
	[113.178.59.119]	[179.0.112.101]	[200.106.93.138]	[58.186.10.38]
	[114.122.71.181]	[179.0.118.162]	[200.110.62.91]	[58.27.133.42]
	[114.130.186.226]	[179.108.16.40]	[200.113.250.139]	[58.27.211.186]
	[115.136.152.136]	[179.19.167.210]	[200.137.65.100]	[60.246.182.201]
	[115.164.119.75]	[179.25.83.156]	[200.152.116.242]	[61.73.66.29]
	[115.164.60.14]	[179.26.238.233]	[200.215.224.212]	[62.114.107.72]
	[115.84.71.195]	[179.6.164.162]	[200.219.51.239]	[62.73.122.178]
	[115.96.213.48]	[179.6.164.187]	[200.57.28.10]	[66.81.175.79]
	[116.107.150.103]	[179.6.168.235]	[200.6.83.143]	[69.80.11.13]
	[116.108.145.216]	[179.6.48.98]	[200.7.123.104]	[77.172.201.22]
	[116.127.67.154]	[179.6.89.148]	[200.71.57.101]	[77.23.248.125]
	[116.96.47.113]	[179.7.225.183]	[200.88.213.54]	[77.249.204.167]
	[116.97.107.29]	[179.7.226.84]	[200.88.26.110]	[78.110.191.172]
	[117.102.63.25]	[179.96.187.127]	[200.9.30.233]	[78.188.185.118]
	[117.99.61.196]	[179.97.123.213]	[201.131.182.11]	[79.146.225.170]
	[118.179.23.89]	[180.231.200.244]	[201.131.237.62]	[79.153.212.235]
	[118.36.88.3]	[181.117.93.181]	[201.141.127.118]	[79.176.104.138]
	[119.152.242.157]	[181.118.72.55]	[201.160.167.45]	[79.181.126.168]
	[119.156.79.1]	[181.13.110.242]	[201.17.159.122]	[79.9.84.213]
	[121.172.119.132]	[181.16.124.239]	[201.203.6.32]	[80.106.232.206]
	[122.172.87.27]	[181.169.205.212]	[201.206.180.22]	[80.208.69.199]
	[122.180.84.172]	[181.188.125.146]	[201.212.243.46]	[80.233.60.150]
	[122.50.225.3]	[181.20.111.41]	[201.213.127.60]	[80.245.97.136]
	[123.214.8.238]	[181.209.231.237]	[201.240.205.208]	[81.100.81.73]
	[123.51.77.73]	[181.29.253.223]	[202.238.19.139]	[82.53.44.233]
	[125.185.32.150]	[181.51.194.217]	[202.29.68.110]	[82.61.42.150]
	[125.235.238.41]	[181.59.3.115]	[203.189.116.227]	[82.81.44.166]
	[128.201.0.219]	[181.64.93.128]	[204.16.9.15]	[83.144.164.52]
	[128.201.134.62]	[181.66.165.128]	[204.199.128.206]	[84.118.65.61]
	[131.0.32.146]	[181.91.175.100]	[206.0.93.240]	[84.220.85.207]
	[131.255.37.170]	[182.185.137.216]	[210.218.182.214]	[84.223.46.24]
	[133.32.155.5]	[182.48.225.177]	[210.23.160.249]	[85.67.0.15]
	[134.101.186.153]	[182.76.130.98]	[211.105.145.78]	[87.116.132.188]
	[138.117.99.18]	[183.182.114.91]	[211.211.81.42]	[87.116.135.198]

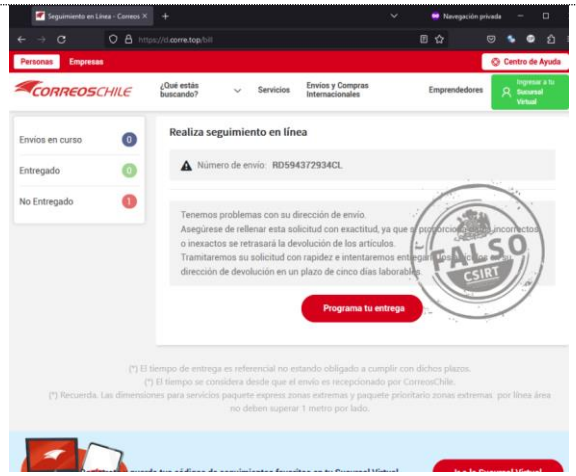
	[138.118.232.116]	[183.78.114.44]	[211.224.193.236]	[87.126.208.75]
	[138.185.156.244]	[185.144.120.207]	[212.104.225.127]	[87.126.55.112]
	[138.36.41.185]	[185.167.93.226]	[212.39.75.195]	[88.10.160.216]
	[138.94.87.242]	[185.189.23.123]	[212.5.158.12]	[88.130.146.236]
	[138.97.199.175]	[185.19.76.108]	[213.145.202.150]	[88.156.132.120]
	[138.99.70.110]	[185.209.236.145]	[213.184.110.236]	[88.53.99.253]
	[138.99.8.17]	[185.228.142.40]	[213.29.243.76]	[89.134.13.191]
	[14.100.46.32]	[185.233.247.17]	[213.81.182.26]	[89.134.23.87]
	[14.162.152.225]	[185.234.234.137]	[216.48.99.165]	[89.134.31.252]
	[14.179.116.88]	[186.12.5.104]	[217.52.225.9]	[89.152.142.228]
	[14.191.131.171]	[186.130.63.137]	[217.64.97.61]	[89.152.234.205]
	[14.191.169.143]	[186.137.172.110]	[219.96.60.53]	[89.153.239.52]
	[14.191.20.134]	[186.15.84.247]	[220.152.112.102]	[89.153.3.109]
	[14.231.116.250]	[186.150.172.222]	[222.251.178.94]	[89.154.40.40]
	[14.46.90.62]	[186.208.22.108]	[223.178.212.152]	[89.204.139.120]
	[14.52.22.182]	[186.211.102.122]	[223.233.83.94]	[89.230.34.41]
	[140.213.218.153]	[186.216.60.159]	[24.233.236.25]	[89.247.162.249]
	[140.213.218.74]	[186.218.42.28]	[27.57.112.210]	[90.153.31.83]
	[141.237.124.169]	[186.219.212.243]	[27.64.191.189]	[91.191.24.114]
	[142.247.224.74]	[186.225.188.5]	[27.68.69.237]	[91.235.160.16]
	[143.0.16.72]	[186.52.243.32]	[27.77.76.48]	[91.92.115.162]
	[144.64.49.209]	[186.52.77.6]	[27.78.229.236]	[91.93.162.66]
	[146.196.35.69]	[186.53.19.245]	[27.79.236.10]	[92.194.241.109]
	[147.235.192.138]	[186.54.219.214]	[31.0.21.107]	[92.209.97.54]
	[148.0.113.191]	[186.54.25.78]	[31.217.1.15]	[92.212.11.229]
	[148.255.249.46]	[186.55.93.160]	[31.217.2.177]	[92.85.150.88]
	[148.71.151.121]	[186.7.192.106]	[31.22.50.20]	[93.67.103.61]
	[149.62.205.175]	[186.7.70.11]	[31.5.148.157]	[94.112.250.3]
	[151.15.93.10]	[186.82.87.153]	[36.95.143.117]	[94.128.153.238]
	[151.192.148.82]	[187.110.233.27]	[37.174.46.14]	[94.183.153.233]
	[151.237.13.77]	[187.111.139.10]	[37.248.169.127]	[94.189.135.28]
	[151.253.243.196]	[187.180.190.39]	[37.248.253.35]	[94.200.187.30]
	[151.46.64.142]	[187.181.209.91]	[37.248.43.46]	[94.248.191.51]
	[151.52.47.66]	[187.22.252.199]	[37.249.159.194]	[94.62.174.250]
	[151.63.44.145]	[187.23.209.111]	[37.76.43.198]	[95.223.107.97]
	[151.72.203.192]	[187.250.195.238]	[37.97.36.188]	[95.42.35.54]
	[154.115.69.2]	[187.38.60.93]	[38.25.17.232]	[95.57.109.12]
	[154.121.73.253]	[187.62.47.136]		
	Enlace para revisar IoC:			
	https://www.csirt.gob.cl/alertas/8fph23-00846-01/			



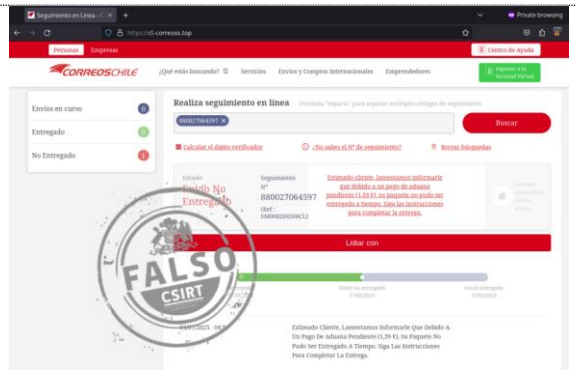
CSIRT alerta de nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00847-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
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/8fph23-00847-01/	



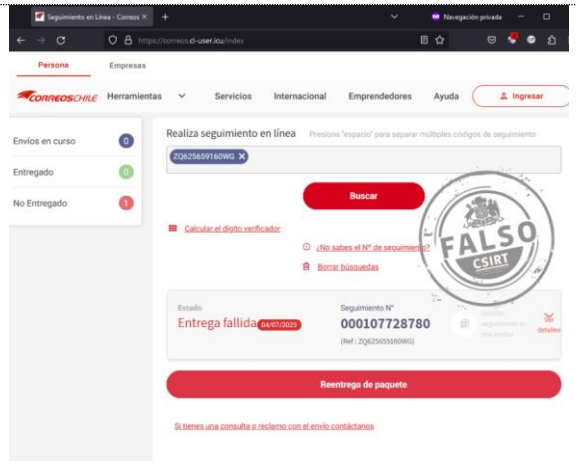
CSIRT alerta de nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00848-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL sitio falso	
http://corr–eos[.]top	
Dirección IP sitio falso	
[47.253.50.251]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00848-01/	



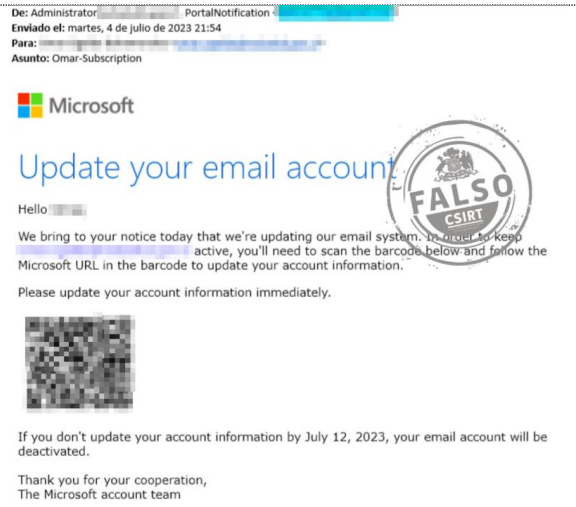
CSIRT alerta de nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00849-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 julio, 2023
Última revisión	5 julio, 2023
Indicadores de compromiso	
URL redirección	
https://qrco.de/be8Dce	
URL sitio falso	
https://cl.corre[.]top/bill	
Dirección IP sitio falso	
[49.51.142.129]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00849-01/	



CSIRT alerta de nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00850-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL redirección	
https://is[.]gd/wFVBsp	
URL sitio falso	
https://cl-correoss[.]top/	
Dirección IP sitio falso	
[155.94.235.71]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00850-01/	



CSIRT alerta de nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00851-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL redirección	
https://cutt.ly/lwyCXejn	
URL sitio falso	
https://correos.cl-user[.]icu/index	
Dirección IP sitio falso	
[49.51.142.129]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00851-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a Microsoft	
Alerta de seguridad cibernética	8FPH23-00852-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://bafybeiaa34zcdtbd5gpnkmcxb7rtixfhupgr27vfo4o3zyqo6zgojyysqe.ipfs.cf-ipfs.com/zoom1.html	
Dirección IP sitio falso	
N/D	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00852-01/	

3. Vulnerabilidades

CSIRT comparte información de nuevas vulnerabilidades en Google Chrome 114	
Alerta de seguridad cibernética	9VSA23-00855-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 junio, 2023
Última revisión	30 junio, 2023
CVE	
CVE-2023-3420 CVE-2023-3421 CVE-2023-3422	
Fabricante	
Google	
Productos afectados	
Google Chrome 114.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00855-01/	

CSIRT alerta de vulnerabilidad en Cisco ACI Multi-Site CloudSec	
Alerta de seguridad cibernética	9VSA23-00856-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023
CVE	
CVE-2023-20185	
Fabricante	
Cisco	
Productos afectados	
Cisco Nexus 9332C, 9364C, y 9500 spine switches (los últimos equipados con Cisco Nexus N9K-X9736C-FX Line Card), solo si están en modo ACI.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00856-01/	

CSIRT comparte información de vulnerabilidades incluidas en Boletín de Seguridad de Android para julio 2023	
Alerta de seguridad cibernética	9VSA23-00857-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 julio, 2023
Última revisión	6 julio, 2023

CVE

CVE-2021-0948	CVE-2023-21243	CVE-2023-2136
CVE-2021-29256	CVE-2023-21245	CVE-2023-21629
CVE-2022-28350	CVE-2023-21246	CVE-2023-21631
CVE-2022-42703	CVE-2023-21247	CVE-2023-21672
CVE-2023-20754	CVE-2023-21248	CVE-2023-22386
CVE-2023-20755	CVE-2023-21249	CVE-2023-22387
CVE-2023-20910	CVE-2023-21250	CVE-2023-22667
CVE-2023-20918	CVE-2023-21251	CVE-2023-24851
CVE-2023-20942	CVE-2023-21254	CVE-2023-24854
CVE-2023-21087	CVE-2023-21255	CVE-2023-25012
CVE-2023-21145	CVE-2023-21256	CVE-2023-26083
CVE-2023-21238	CVE-2023-21257	CVE-2023-28147
CVE-2023-21239	CVE-2023-21261	CVE-2023-28541
CVE-2023-21240	CVE-2023-21262	CVE-2023-28542
CVE-2023-21241		

Fabricante

Google

Productos afectados

Dispositivos Android.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00857-01/

4. Concientización

Ciberconsejos para el uso seguro del correo electrónico

El correo electrónico es un canal de comunicación muy importante. A través de esta plataforma, las personas trabajan, guardan información, se registran en sitios web, contratan servicios, etc. ¿Cómo cuidar tu información y usar de forma segura tu correo electrónico? Te contamos aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-uso-seguro-correo-electronico/

CUIDADO | Nueva campaña de phishing por SMS (smishing) que suplanta a CorreosChile

Debemos tener mucho cuidado con las estafas y ataques de phishing que circulan en internet. Una de las más recientes y que se ha difundido mucho en todo el país durante esta última semana es la que pueden ver en las imágenes, que suplanta a CorreosChile. Si recibes estos mensajes de texto u otros similares, y también para el caso de emails sospechosos, te recomendamos siempre que no hagas clic.

Más información sobre esta campaña de smishing:

https://www.csirt.gob.cl/alertas/8fph23-00847-01/
https://www.csirt.gob.cl/alertas/8fph23-00848-01/
https://www.csirt.gob.cl/alertas/8fph23-00849-01/

Si tienes dudas y crees que un mensaje pueda ser legítimo, contacta directamente a la institución aludida a través de su teléfono oficial, nunca haciendo clic o respondiendo al mensaje sospechoso.

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.

- Rodrigo Cortés
- Nelson Silva
- Luis Eduardo Pineda Rebolledo
- Eduardo Hurtado Palacios
- Josué Nicolás Leiva Poblete
- Sugy Nam
- Patricio Guzmán
- Miguel Gallegos
- Gonzalo Andrés Carvajal Torres
- Pablo Araya del Pino
- Claudio Felipe Pontigo Puentes
- Fernando Flores Tobar
- Claudia Alejandra Pérez Hernández
- Franco Alexis Gallegos Vallejos
- María José Fuentes Urrutia

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.07 18:23:21 -04'00'