CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | Nº 180

SEMANA DEL 9 AL 15 DE DICIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

65

Las mitigaciones son útiles en productos de Google.

IP INFORMADAS

97

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

URL ADVERTIDAS

94

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

5

Asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

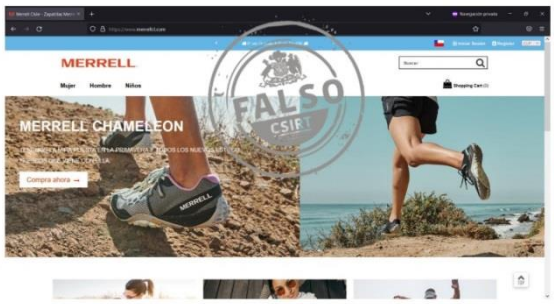
1. Malware

CSIRT alerta de phishing con malware que suplanta a Pypco	
Alerta de seguridad cibernética	2CMV22-00392-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2022
Última revisión	13 de diciembre de 2022
Indicadores de compromiso	
Asunto	
FW: error de número de cuenta y pago devuelto	
Correo de Salida	
pagos.culiacan@pypco.com.mx	
SHA256	
f438c543b7b5c3b45f2a6c132bad071b49bd8c8a581a73fa75eb5c581ece267d 27fcd49dd8387a91b82b9af142abeddf6caf2b37188b725132468aee0cec8f06	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00392-01/	
https://www.csirt.gob.cl/media/2022/12/2CMV22-00392-01.pdf	

CSIRT alerta de campaña de phishing con malware, que suplanta a Scania	
Alerta de seguridad cibernética	2CMV22-00393-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de diciembre de 2022
Última revisión	15 de diciembre de 2022
Indicadores de compromiso	
Asunto	
SOLICITUD DE COTIZACIÓN	
Correo de Salida	
tomas.jorquera@scania.com	
SHA256	
63be3965b1f68ab7d135f8c5bb3174400b89e6fba7f6bd7c5c783fdce7c5d1ba 04b74d509ebe0ab8af4e937aca17c019cc7af5c8b3f5a94fedd20c458a6b58ca e3a02800fff28a44de874d73e78803f316a637cc970412eedf4662c222a6e9e	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00393-01/	
https://www.csirt.gob.cl/media/2022/12/2CMV22-00393-01.pdf	

2. Sitios fraudulentos

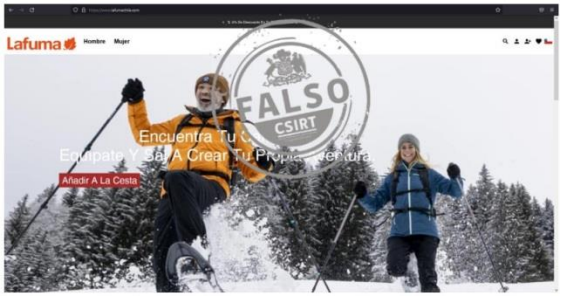
Imagen del sitio



CSIRT alerta de 44 páginas fraudulentas que suplantan a conocidas marcas	
Alerta de seguridad cibernética	8FFR22-01153-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
www.schutzchile[.]com/	
https://www.merrellchile[.]com/	
www.drschollschile[.]com/	
www.propetchile[.]com/	
www.goldengooseoutletchile[.]com/	
www.goldengoosemchile[.]com	
www.lowaenchile[.]com/	
https://www.salomonchilecl[.]com/	
https://www.alohaschile[.]com/	
www.furla-chile.com/	
www.lowachilecl[.]com/	
www.costadelmarchile[.]com/	
www.obozchile[.]com/	
www.oliverpeopleschile[.]com/	
www.persolchile[.]com/	
www.mauijimchile[.]com/	
www.zapatosmephistochile[.]com	
www.merrellcl[.]com/	
https://www.pumachilecl[.]com/	
www.lasportiva-chile[.]com/	
www.pleaserchile[.]com/	
www.ryderwearchile[.]com/	
www.ropaobeychile[.]com/	
groundiesoutletchile[.]com/	
https://www.g-starchile[.]com/	
www.miumiuchile[.]com/	
www.chile-reebok.com/	
https://www.volcom-chile[.]com/	
outlettimberland-chile[.]com	
https://www.tiendaskechersonlinechile[.]com/	
www.aloyoga-chile[.]com/	
https://www.botashunterchile[.]cl/	
www.quiksilverchile[.]com/	
www.gantchile[.]com/	
www.jordanofertachile[.]com/	
www.nobullchiletiendas[.]com/	
www.hunterbootchile[.]com/	
www.sebagochileoutlet[.]com/	
https://www.michaelkorschile[.]com/	
www.onrunnerchile[.]com/	
www.tiendapumachile[.]com/	
www.woolrichchile[.]com/	

	https://www.eccooutletchile[.]com/ www.palmangels-chile[.]com/
	Dirección IP
	[5.157.8.245] [196.240.121.131] [5.157.8.242] [196.240.121.130] [5.157.8.221] [196.196.197.225] [5.157.8.214] [196.196.197.190] [5.157.8.198] [196.196.197.184] [5.157.8.198] [196.196.197.170] [5.157.59.55] [196.196.197.123] [5.157.42.92] [196.196.194.183] [5.157.42.162] [196.196.194.157] [5.157.42.114] [196.247.55.111] [196.247.61.54] [196.242.16.57] [196.247.61.249] [196.242.16.49] [196.247.61.248] [196.242.16.14] [196.247.61.238] [196.242.16.14] [196.247.61.235] [196.240.45.46] [196.247.61.210] [196.196.57.44] [196.247.61.16] [196.196.57.14] [196.247.59.132] [165.231.36.57] [196.247.55.118] [165.231.36.46] [196.247.55.111] [165.231.36.16] [196.242.16.57] [196.240.121.200] [196.242.16.49] [196.240.121.159] [196.242.16.14] [196.240.121.152] [196.242.16.14] [196.240.121.140] [196.240.45.46] [196.240.121.136] [196.196.57.44] [196.196.57.14] [165.231.36.57] [165.231.36.46]
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/alertas/8ffr22-01153-01/
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01153-01.pdf

Imagen del sitio



CSIRT alerta de 12 web falsas que suplantan a diversas marcas	
Alerta de seguridad cibernética	8FFR22-01154-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
www.zapatoseccochile[.]com/ www.caterpillarenchile[.]com/ www.champion-chile[.]com/ www.fila-chile[.]com/ www.osiriszapatillaschile[.]com/ www.doctormartenchile[.]com/ www.lafumachile[.]com https://www.danneroutletchile[.]com/ www.ua-chile[.]com www.vessichile[.]com/ https://www.reebokchile-outlet[.]com/ www.pranachile[.]com/	
Dirección IP	
[196.245.249.94] [196.244.47.154] [196.245.249.87] [196.196.38.178] [196.245.249.83] [196.196.38.155] [196.245.249.78] [165.231.154.44] [196.245.249.66] [196196206150] [196.244.47.79] [165.231.152.143]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01154-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01154-01.pdf	

Imagen del sitio

CSIRT alerta de nueve sitios fraudulentos que suplantan a marcas como Psycho Bunny y Amphora	
Alerta de seguridad cibernética	8FFR22-01155-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
www.koiyu[.]site www.clothingyoung[.]online www.billeterascl[.]online/ www.vsetidonline[.]shop/ www.bellearopaes[.]shop/ www.clothingpromos[.]online/ www.violatieon[.]shop/ https://www.casacamas[.]store/ https://www.psychobunnychile[.]com/	
Dirección IP	
[167.160.3.15] [23.252.71.157] [23.252.71.100] [23.252.68.238] [198.55.28.3] [167.160.3.25] [162.222.89.169] [107.150.171.101]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01155-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01155-01.pdf	

Imagen del sitio

CSIRT alerta de sitios fraudulentos que suplantan a empresas como Doite	
Alerta de seguridad cibernética	8FFR22-01156-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.ropamujers[.]store/	
deitecl[.]com	
Dirección IP	
[5.255.62.156]	
[185.212.172.116]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01156-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01156-01.pdf	

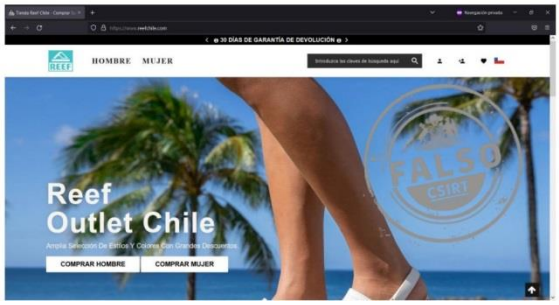
Imagen del sitio		
	**CSIRT alerta de cinco sitios web fraudulentos que suplantan a marcas como Lotto y Reef**	
	Alerta de seguridad cibernética	8FFR22-01157-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	12 de diciembre de 2022
	Última revisión	12 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	www.reefchile[.]com/	
	www.gymsharkchilestore[.]com/	
	www.tommyhilfigerchileoutlet[.]com/	
	www.lottochile[.]com/	
	www.louboutinchile[.]com/	
	Dirección IP	
	[104.160.4.254]	
	[104.160.4.251]	
	[196.196.231.99]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01157-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01157-01.pdf	

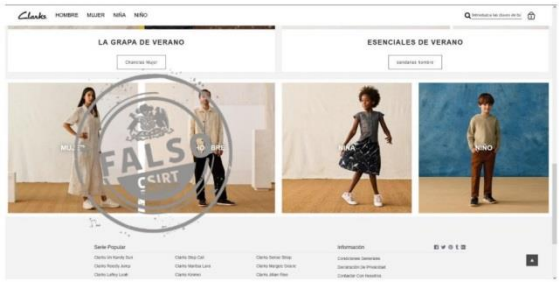
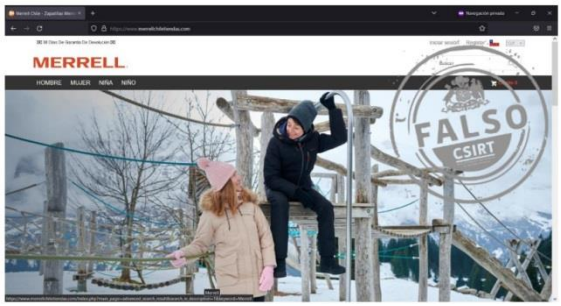
Imagen del sitio		
	**CSIRT alerta ante página fraudulenta que suplanta a Clarks**	
	Alerta de seguridad cibernética	8FFR22-01158-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	12 de diciembre de 2022
	Última revisión	12 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	https://www.clarks-cl.com/	
	Dirección IP	
	[172.67.178.111]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01158-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01158-01.pdf	

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta a Merrell	
Alerta de seguridad cibernética	8FFR22-01159-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.merrellchiletiendas[.]com/	
Dirección IP	
[172.67.178.111]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01159-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01159-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta a Doite	
Alerta de seguridad cibernética	8FFR22-01160-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2022
Última revisión	12 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
doitechile[.]shop	
Dirección IP	
[103.224.182.249]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01160-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01160-01.pdf	

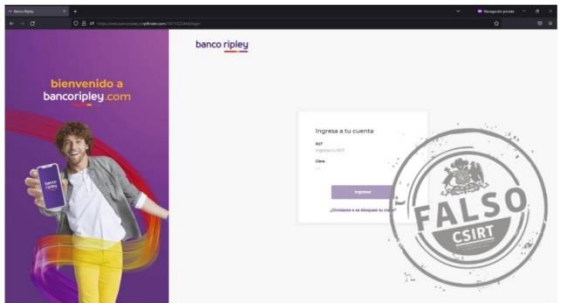
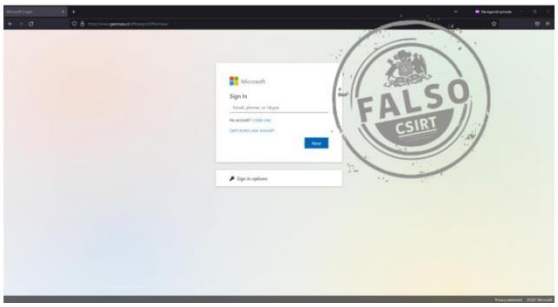
Imagen del sitio		
	**CSIRT alerta de un sitio fraudulento que suplanta al Banco Ripley**	
	Alerta de seguridad cibernética	8FFR22-01161-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	14 de diciembre de 2022
	Última revisión	14 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	https://web.bancoripley.cl.rplfinder[.]com/1671023444/login	
	Dirección IP	
	[163.47.75.82]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01161-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01161-01.pdf	

Imagen del sitio		
	**CSIRT alerta de sitio fraudulento que suplanta a Microsoft**	
	Alerta de seguridad cibernética	8FFR22-01162-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	14 de diciembre de 2022
	Última revisión	14 de diciembre de 2022
	Indicadores de compromiso	
	URL sitio falso	
	https://www.geomass[.]cl/officesign/Officernew/	
	Dirección IP	
	[186.64.114.110]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01162-01/	
	https://www.csirt.gob.cl/media/2022/12/8FFR22-01162-01.pdf	

3. Phishing

Imagen del mensaje	CSIRT alerta de una nueva campaña de phishing por WhatsApp que suplanta a Soprole	
	Alerta de seguridad cibernética	8FPH22-00674-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	9 de diciembre de 2022
	Última revisión	9 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https://subtletyjudicial[.]cn/soprole/tb.php?at=ok1670587908799	
	URL sitio falso	
	https://conchch[.]top/HUqe42Vd/soprole/?_t=1670598649412#1670598651294	
	Dirección IP	
	[104.21.51.84]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00674-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00674-01.pdf	

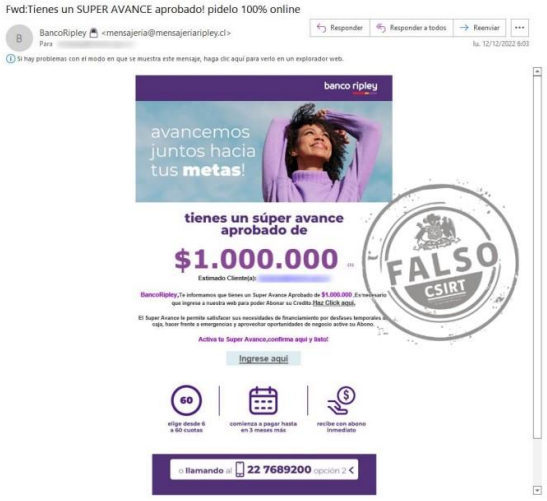
Imagen del mensaje	CSIRT alerta de nueva campaña de phishing por WhatsApp, que suplanta a Banco Ripley	
	Alerta de seguridad cibernética	8FPH22-00675-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	12 de diciembre de 2022
	Última revisión	12 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https://bit[.]ly/3iTAYES?l=www.bancoripley.cl	
	https://sam-tech[.]jp/bancoripley/cuenta-aiuk/	
	URL sitio falso	
	https://web.bancoripley.cl.wedoitbest[.]com.au/1670855814/Login	
	Dirección IP	
	[203.26.41.223]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00675-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00675-01.pdf	

Imagen del mensaje		
	**CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Estado**	
	Alerta de seguridad cibernética	8FPH22-00676-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	12 de diciembre de 2022
	Última revisión	12 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https://ucmstudio[.]info/activacion/cuenta-aotq/	
	URL sitio falso	
	https://celebrafans[.]com/1670857301/imagenes/_personas/home/default.asp	
	Dirección IP	
	[104.21.4.90]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00676-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00676-01.pdf	

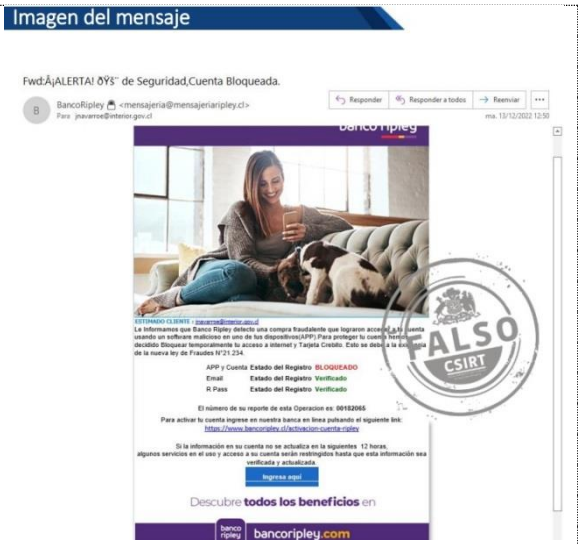
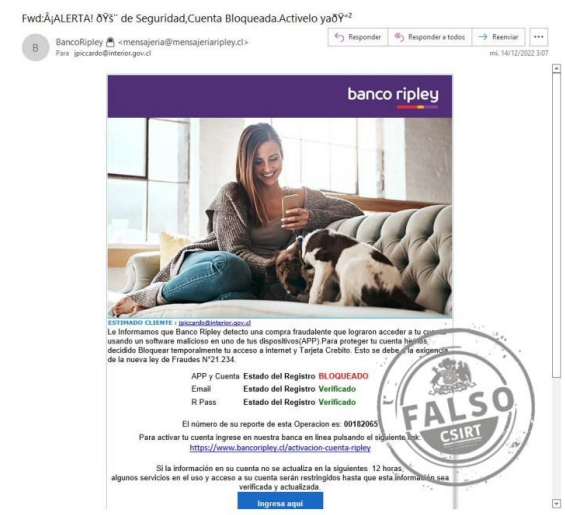
Imagen del mensaje		
	**CSIRT alerta de campaña de phishing que suplanta al Banco Ripley**	
	Alerta de seguridad cibernética	8FPH22-00677-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	13 de diciembre de 2022
	Última revisión	13 de diciembre de 2022
	Indicadores de compromiso	
	URL redirección	
	https://bit[.]ly/3hgrIug?l=www.bancoripley.cl	
	https://sam-tech[.]jp/bancoripley/cuenta-zwgg/	
	URL sitio falso	
	http://web.bancoripley.cl.browshapesmi[.]com/1670947148/login	
	Dirección IP	
	[67.223.118.82]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00677-01/	
	https://www.csirt.gob.cl/media/2022/12/8FPH22-00677-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00678-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2022
Última revisión	13 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://t[.]co/iivqY7ziPk	
https://gecochile[.]com/index/?index=index	
URL sitio falso	
https://santanderchile-personas.kar-growth[.]com/1670953350/portada/personas/home.asp	
Dirección IP	
[198.54.116.206]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00678-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00678-01.pdf	

Imagen del mensaje



CSIRT alerta ante campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00679-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2022
Última revisión	14 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3FsyhSe?l=www.bancoripley.cl	
https://reisdaviau[.]pt/bancoripley/cuenta-gqha/	
URL sitio falso	
https://web.bancoripley.cl.wonthaggicaravans.com.au/1671022251/login	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00679-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00679-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00680-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2022
Última revisión	14 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https://avengerpati[.]com/activacion/cuenta-lkok/	
URL sitio falso	
https://smscotito[.]info/1671031809/imagenes/_personas/home/default.asp	
Dirección IP	
[162.241.60.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00680-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00680-01.pdf	

4. Fuerza Bruta

CSIRT alerta de ataques de fuerza bruta contra el protocolo SMTP	
Alerta de seguridad cibernética	4IIA22-00057-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2022
Última revisión	13 de diciembre de 2022
Indicadores de compromiso	
Direcciones IP	
[199.195.181.154] [85.209.135.176] [176.111.173.54] [198.244.229.220] [141.98.10.236] [79.110.63.196]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iiv22-00057-01/	
https://www.csirt.gob.cl/media/2022/12/4IIV22-00057-01.pdf	

5. Vulnerabilidades

CSIRT alerta de nuevas vulnerabilidades que afectan a varios productos de Cisco		
Alerta de seguridad cibernética	9VSA22-00752-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	13 de diciembre de 2022	
Última revisión	13 de diciembre de 2022	
CVE		
CVE-2022-20968	CVE-2022-20956	CVE-2022-20962
CVE-2022-20867	CVE-2022-3602	CVE-2022-20964
CVE-2022-20868	CVE-2022-3786	CVE-2022-20965
CVE-2022-20922	CVE-2022-20961	CVE-2022-20966
CVE-2022-20943	CVE-2022-20963	CVE-2022-20967
Fabricantes		
Cisco		
Productos afectados		
Cisco Identity Services Engine (ISE) Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, y Cisco Secure Web Appliance Cisco IP Phone 7800 and 8800 Series		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00752-01/		
https://www.csirt.gob.cl/media/2022/12/9VSA22-00752-01-1.pdf		

CSIRT alerta de vulnerabilidad crítica en FortiOS de Fortinet	
Alerta de seguridad cibernética	9VSA22-00753-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	13 de diciembre de 2022
Última revisión	13 de diciembre de 2022
CVE	
CVE-2022-42475	
Fabricantes	
Fortinet	
Productos afectados	
FortiOS 5.0.0 a 7.2.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00753-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00753-01.pdf	

CSIRT comparte las vulnerabilidades entregadas por Microsoft en su Update Tuesday de diciembre	
Alerta de seguridad cibernética	9VSA22-00754-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2022
Última revisión	14 de diciembre de 2022

CVE

CVE-2022-44687	CVE-2022-44704	CVE-2022-44679
CVE-2022-41089	CVE-2022-44699	CVE-2022-44677
CVE-2022-44702	CVE-2022-44691	CVE-2022-44678
CVE-2022-41094	CVE-2022-44698	CVE-2022-44676
CVE-2022-41076	CVE-2022-44697	CVE-2022-44675
CVE-2022-24480	CVE-2022-44696	CVE-2022-44674
CVE-2022-47213	CVE-2022-44695	CVE-2022-44673
CVE-2022-47212	CVE-2022-44694	CVE-2022-44671
CVE-2022-47211	CVE-2022-44693	CVE-2022-44670
CVE-2022-26806	CVE-2022-44692	CVE-2022-44669
CVE-2022-26805	CVE-2022-44690	CVE-2022-44668
CVE-2022-26804	CVE-2022-44689	CVE-2022-44667
CVE-2022-44713	CVE-2022-44683	CVE-2022-44666
CVE-2022-41127	CVE-2022-44682	CVE-2022-41121
CVE-2022-44710	CVE-2022-44681	CVE-2022-41077
CVE-2022-44707	CVE-2022-44680	CVE-2022-41074

Fabricantes

Microsoft

Productos afectados

.NET 6.0
.NET 7.0
.NET Core 3.1
Azure Network Watcher VM Extension
Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
Dynamics 365 Business Central Spring 2019 Update
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.6/4.6.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 Business Central 2020 Release Wave 1
Microsoft Dynamics 365 Business Central 2020 Release Wave 2
Microsoft Dynamics 365 Business Central 2021 Release Wave 1
Microsoft Dynamics 365 Business Central 2021 Release Wave 2
Microsoft Dynamics 365 Business Central 2022 Release Wave 1
Microsoft Dynamics 365 Business Central 2022 Release Wave 2
Microsoft Dynamics NAV 2016

	Microsoft Dynamics NAV 2017 Microsoft Dynamics NAV 2018 Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for Mac Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft Outlook for Android Microsoft SharePoint Enterprise Server 2013 Service Pack 1 Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft Visio 2013 Service Pack 1 (32-bit editions) Microsoft Visio 2013 Service Pack 1 (64-bit editions) Microsoft Visio 2016 (32-bit edition) Microsoft Visio 2016 (64-bit edition) Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10) Microsoft Visual Studio 2022 version 17.0 Microsoft Visual Studio 2022 version 17.2 Microsoft Visual Studio 2022 version 17.4 PowerShell 7.2 PowerShell 7.3 Raw Image Extension Remote Desktop client for Windows Desktop Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2008 for 32-bit Systems Service Pack 2

	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022 Datacenter: Azure Edition Windows Subsystem for Linux (WSL2) Windows Sysmon Windows Terminal for Windows 10 Windows Terminal for Windows 11
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00754-01/
	https://www.csirt.gob.cl/media/2022/12/9VSA22-00754-01.pdf

CSIRT alerta de vulnerabilidad crítica en Citrix ADC y Gateway	
Alerta de seguridad cibernética	9VSA22-00755-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2022
Última revisión	14 de diciembre de 2022
CVE	
CVE-2022-27518	
Fabricantes	
Citrix	
Productos afectados	
Citrix ADC y Citrix Gateway 13.0 anteriores a 13.0-58.32 Citrix ADC y Citrix Gateway 12.1 anteriores a 12.1-65.25 Citrix ADC 12.1-FIPS anteriores a 12.1-55.291 Citrix ADC 12.1-NDcPP anteriores a 12.1-55.291	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00755-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00755-01.pdf	

6. Concientización

Ciberconsejos para compras seguras en Navidad

Ya en diciembre muchas personas comienzan a planificar sus compras navideñas. Si este año preferirás los canales digitales, el CSIRT de Gobierno entrega los siguientes para comprar de forma segura y así evitar ser víctima de alguna estafa o fraude cibernético.

Ver video: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-navidad/

Ciberdiccionario Volumen 25

En esta ocasión, en el ciberdiccionario del CSIRT de Gobierno revisamos los conceptos de ciberinteligencia y cibermercenario, además de aprender qué son los SOC y la red TOR.

7. 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 los sitios web que se ingresen sean los oficiales.

8. 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.

- Gerson Palacios
- Vicente Raty
- Claudia Enríquez
- Catalina Ulloa
- Cristopher Pérez