

SEMANA EN CIFRAS

PARCHES COMPARTIDOS

9

Las mitigaciones son útiles en productos de Cisco, Fortinet y VMware.



IP INFORMADAS

20

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



URL ADVERTIDAS

28

Asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

2

Asociadas a múltiples campañas de phishing con archivos que contienen malware



			7 : :		
	os				
	\ \				
	: II				
	es y buenas prácticas				
Muro de la Fama	ı				
	1011	. A. W. L.		7.5	TIE.
+			+1		
E .		= -			
	100				
+ , ,			+ +		
	/#\\				
	////		1		
•	////				
	////				
	- ////				

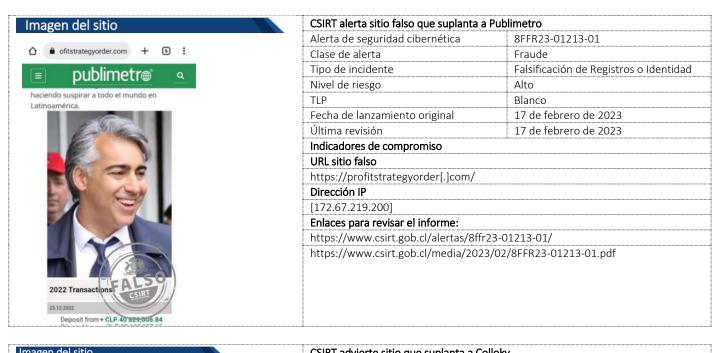
•

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

1. Sitios fraudulentos





CSIRT advierte sitio que suplanta a Col	loky					
Alerta de seguridad cibernética	8FFR23-01214-01					
Clase de alerta	Fraude					
Tipo de incidente	Falsificación de Registros o Identidad					
Nivel de riesgo	Alto					
TLP	Blanco					
Fecha de lanzamiento original	17 de febrero de 2023					
Última revisión	17 de febrero de 2023					
Indicadores de compromiso						
URL sitio falso						
https://colleky-clothing.sitey[.]me/						
Dirección IP						
[104.18.135.142]						
Enlaces para revisar el informe:						
https://www.csirt.gob.cl/alertas/8ffr2	https://www.csirt.gob.cl/alertas/8ffr23-01214-01/					
https://www.csirt.gob.cl/media/2023/02/8FFR23-01214-01-1.pdf						

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

magen del sitio				CSIRT advierte sitio web que suplanta a Colloky				
					Alerta de seguridad cibernética	8FFR23-01215-01		
© ZJPATILIAS	× +		∨ 🔛 Navegaci	on privada — 🔲 🗵	Clase de alerta	Fraude		
← → C	https://www.dewittrapebn.shop/sa	patilas-I-ODAwMjAwODk=-MjAyMzAj	MTWODMONDQ40TQy.ht 🏠	© ≜ එ ≅ B Rastreo de	Tipo de incidente	Falsificación de Registros o Identidad		
Colloky			Q	•	Nivel de riesgo	Alto		
BEBÉ	IIÑA NIÑO	ZAPATOS	ROPA ACCESO	RIOS NOVEDADI	TLP	Blanco		
10% DCTO	1 / 1939	11	ENVÍIO GRATIS A PARTIR	DE \$33.506	Fecha de lanzamiento original	17 de febrero de 2023		
EBÉ Y	(1-2) EAL	50	3 4 5 > >>	Recomendados	Última revisión	17 de febrero de 2023		
CSIRT			Indicadores de compromiso					
APATOS ^	1	Strain .			URL sitio falso			
ZAPATILLAS BOTAS Y BOTINES ZAPATOS					https://www.dewittrapebn[.]shop/			
REINAS Y BALLERINAS SANDALIAS Y ALPARGATAS					Dirección IP			
	Zapatilla De Niño Mickey Astronauta Cambia De Color Co \$6.893 \$35,420	Zapatilia De Niño Mickey Astronauta Cambia De Color Co \$6.127 \$12.50\$	Zapatilia De Niño Marvel Comic Azal (28 A 38) \$6.893 \$32.335	Zapatilla Deportiva De Niñ Baja Gris (21 A 27) \$3.829 \$22.018	[167.160.3.16]			
Ver Todo					Enlaces para revisar el informe:			
CCESORIOS ~	A Para		100	400	https://www.csirt.gob.cl/alertas/8ffi	r23-01215-01/		
DVEUADES	EVELODES STATE OF THE STATE OF			https://www.csirt.gob.cl/media/2023/02/8FFR23-01215-01-1.pdf				
	Zapatilia Deportiva De Niño Caña Raia Anii (28 A 28)	Zagatilia Deportiva De Niño Caña Reia Aral (11 A 27)	Zapatina Urbana De Niña Tipo Chindra Blanca (38 A 21)	Zapatilla Deportiva De Niñi Rais Neces (71 à 77)				



CSIRT alerta página web que suplanta	a Colloky					
Alerta de seguridad cibernética	8FFR23-01216-01					
Clase de alerta	Fraude					
Tipo de incidente	Falsificación de Registros o Identidad					
Nivel de riesgo	Alto					
TLP	Blanco					
Fecha de lanzamiento original	17 de febrero de 2023					
Última revisión 17 de febrero de 2023						
Indicadores de compromiso						
URL sitio falso						
https://www.colloky-cl[.]shop/						
Dirección IP						
[172.67.189.111]						
Enlaces para revisar el informe:						
https://www.csirt.gob.cl/alertas/8ffr	23-01216-01/					
https://www.csirt.gob.cl/media/2023/02/8FFR23-01216-01.pdf						



Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

magen	del sitio				CSIRT advierte sitio que suplanta a Ca	aterpillar
Catalo	A http://www.rathout.onfine			Nevegación privada	Alerta de seguridad cibernética	8FFR23-01217-01
S CLP +					Clase de alerta	Fraude
CAT		\	q	. ₩	Tipo de incidente	Falsificación de Registros o Identidad
HOM	ISS OF THE END	MIJER	ACCESORIOS ENVIIO GRATIS A PART	CAT X 1137.	Nivel de riesgo	Alto
Inicio / Hombre /	Catago				TLP	Blanco
HOMBRE Calzado	The state of the s	ee e 1	1 2 3 4 5 > >>	Recomendados ~	Fecha de lanzamiento original	20 de febrero de 2023
Zapetifes Sociees V Socoose					Última revisión	20 de febrero de 2023
Sequidad	Sepurited Sepurited		Indicadores de compromiso			
Ver Tade Vestuario Accesorios					URL sitio falso	
Colecciones Ver Todo	Zaptilla Quest Runner Homb	S9,990 pzz.eso	Zapatitia Hombre Reactor \$13,990 pps.app	\$7,990 Saleso	https://www.catboot[.]online/	
MUJER ACCESORIOS	*		7		Dirección IP	
CAT X DBZ				- 4	[107.150.173.211]	
	A Property of the Parks				Enlaces para revisar el informe:	
	ZAPATILLA HEX TOUGH HOS	IERE Zapatilla Quest Mid Hombre	Zaptilia Hex Tough Hombre	Zapatila Ventura Hiker Lo	https://www.csirt.gob.cl/alertas/8ffr	23-01217-01/
				Horace	https://www.csirt.gob.cl/media/202	3/02/8FFR23-01217-01.pdf



CSIRT alerta de página web que supla	nta a Vans				
Alerta de seguridad cibernética	8FFR23-01218-01				
Clase de alerta	Fraude				
Tipo de incidente	Falsificación de Registros o Identidad				
Nivel de riesgo	Alto				
TLP	Blanco				
Fecha de lanzamiento original	20 de febrero de 2023				
Última revisión	20 de febrero de 2023				
Indicadores de compromiso					
URL sitio falso					
https://www.vansoutletcl[.]shop/					
Dirección IP					
[172.67.147.143]					
Enlaces para revisar el informe:					
https://www.csirt.gob.cl/alertas/8ffr23-01218-01/					
https://www.csirt.gob.cl/media/2023/02/8FFR23-01218-01-1.pdf					



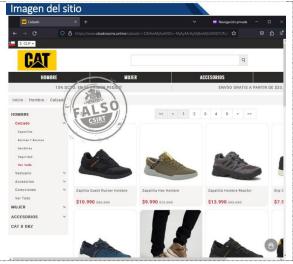
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

ABCDIN) Missies Ofertes y De. X +			Navegación privada			
← → C PA HIDELING	balin.com		☆	•	9 0	I
= abcdin	Buscar			Q	פק	
CSIRI	facilità e dia mana de anni					
55	lanzamientos Más vendidos	-745	- 0			
	50° 4K				D D	
LED Samsung 60° AU7000 4K UHD Smart TV \$189.980-\$89.990	LED 50° AU7000 4K UHD Smart TV \$159,000 \$99,990		dora secadora 11 ₃ \$189.990 \$49.99 0			
					-	

CSIRT alerta sitio web falso de ABCDIN							
Alerta de seguridad cibernética	8FFR23-01219-01						
Clase de alerta	Fraude						
Tipo de incidente	Falsificación de Registros o Identidad						
Nivel de riesgo	Alto						
TLP	Blanco						
Fecha de lanzamiento original	20 de febrero de 2023						
Última revisión 20 de febrero de 2023							
Indicadores de compromiso	Indicadores de compromiso						
URL sitio falso							
https://seguro-abcdin[.]com/	https://seguro-abcdin[.]com/						
Dirección IP	Dirección IP						
[23.227.38.68]							
Enlaces para revisar el informe:							
https://www.csirt.gob.cl/alertas/8ffr23	3-01219-01/						
https://www.csirt.gob.cl/media/2023/02/8FFR23-01219-01.pdf							



CSIRT advierte página web que suplanta	a Caterpillar						
Alerta de seguridad cibernética	8FFR23-01220-01						
Clase de alerta Fraude							
Tipo de incidente	Falsificación de Registros o Identidad						
Nivel de riesgo	Alto						
TLP	Blanco						
Fecha de lanzamiento original	21 de febrero de 2023						
Última revisión 21 de febrero de 2023							
Indicadores de compromiso	Indicadores de compromiso						
URL sitio falso							
https://www.cloakrooms[.]online/							
Dirección IP							
[23.252.68.242]							
Enlaces para revisar el informe:							
https://www.csirt.gob.cl/alertas/8ffr23-	https://www.csirt.gob.cl/alertas/8ffr23-01220-01/						
https://www.csirt.gob.cl/media/2023/02/8FFR23-01220-01.pdf							

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562)

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

						Navegación privada	
	0 8	https://www.zaç	atillaskedschile.com/ho			□ ☆	
	Envio Gra	stuito A Partir De \$	95000	≜ NC	IAR SESIÓN 🆀 RE	GISTER L	
Keds	Hombre	Mujer	Niña Niño	4.	Buscar	Q	F (0)
Casa / Hombre		1	A.	pho			
CATEGORÍAS	^	Mostrando 1 24	-115				1 2 >
■ Hombre □ Zapatitas		-					
Paris Paris				5	0000	GGGG	000
COLECCIÓN	^						
Royal Plus(5) Royal Lo(16)			ds Royal Hi Blancas Chile 20084B75		al Hi Leuther Blancat hile \$0,386H50	Zapatillas Keds Royal Hombre Chile	
Royal H(5)		\$40,696	2 Colores	\$51,004	2 Colores	\$51,004	2 Colores
COLORES	^	-		_		_	
• • •	•	43	Show.	3)	and the same of th	ago,	
TALLA	_						

CSIRT alerta de sitio web falso de Ked	S					
Alerta de seguridad cibernética	8FFR23-01221-01					
Clase de alerta	Fraude					
Tipo de incidente	Falsificación de Registros o Identidad					
Nivel de riesgo	Alto					
TLP	Blanco					
Fecha de lanzamiento original	21 de febrero de 2023					
Última revisión	21 de febrero de 2023					
Indicadores de compromiso	Indicadores de compromiso					
URL sitio falso						
https://www.zapatillaskedschile[.]com/						
Dirección IP						
[104.21.31.126]						
Enlaces para revisar el informe:	Enlaces para revisar el informe:					
https://www.csirt.gob.cl/alertas/8ffr2	https://www.csirt.gob.cl/alertas/8ffr23-01221-01/					
https://www.csirt.gob.cl/media/2023/02/8FFR23-01221-01.pdf						



CSIRT informa de página web que supla	nta al Banco Santander					
Alerta de seguridad cibernética	8FFR23-01222-01					
Clase de alerta Fraude						
Tipo de incidente	Falsificación de Registros o Identidad					
Nivel de riesgo	Alto					
TLP	Blanco					
Fecha de lanzamiento original	22 de febrero de 2023					
Última revisión 22 de febrero de 2023						
Indicadores de compromiso	Indicadores de compromiso					
URL sitio falso						
https://coordenadas[.]buzz/santa.php						
https://coordenadasbloqueada[.]buzz/						
https://bancosantander-cl.chile-						
personas[.]buzz/1677006305/portada/personas/home.asp						
Dirección IP						
[104.21.6.151]						
Enlaces para revisar el informe:	Enlaces para revisar el informe:					
https://www.csirt.gob.cl/alertas/8ffr23	-01222-01/					
https://www.csirt.gob.cl/media/2023/02/8FFR23-01222-01.pdf						

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562)

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

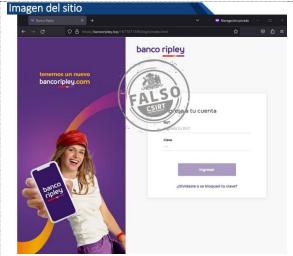
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

■ Lippi Outdoor - Sitio Oficial - □ × +		✓ Mavegación privada — □
← → C O B https://ww	wouldooflopishop	☆ ⊚ {
FA	LS OT rekking	
Chaqueta Niña Shelter B-Dry Hoody Uva Lippi - Morado \$27390 \$24.498	Roca -7 Down Sleeping Bag Lippi - Cris \$799.890 \$44.999	Mochila Roca 60 Backpack Negro V20 Lippi - Negro 5330990 \$35.999
9577370 \$24,430		

CSIRT advierte sitio web falso de Lippi		
Alerta de seguridad cibernética	8FFR23-01223-01	
Clase de alerta	Fraude	
Tipo de incidente	Falsificación de Registros o Identidad	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	22 de febrero de 2023	
Última revisión	22 de febrero de 2023	
Indicadores de compromiso		
URL sitio falso https://www.outdoorlippi[.]shop/ Dirección IP [172.67.193.230] Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr23-01223-01/ https://www.csirt.gob.cl/media/2023/02/8FFR23-01223-01.pdf		



CSIRT alerta página web falsa que suplanta al Banco Ripley			
Alerta de seguridad cibernética	8FFR23-01224-01		
Clase de alerta	Fraude		
Tipo de incidente	Falsificación de Registros o Identidad		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	22 de febrero de 2023		
Última revisión	22 de febrero de 2023		
Indicadores de compromiso			
URL sitio falso			
https://bancoripley[.]top/ https://bancoripley[.]top/1677071590/login/index.html Dirección IP [104.21.28.160] Enlaces para revisar el informe:			
		https://www.csirt.gob.cl/alertas/8ffr23	-01224-01/
		https://www.csirt.gob.cl/media/2023/02/8FFR23-01224-01-1.pdf	



Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

Imagen del sitio		CSIRT advierte sitio falso que suplant	a al Banco Ripley
■ Bance Ripley × + ← → C ○ △ https://web.bancoripley.d.ngyokon		Alerta de seguridad cibernética	8FFR23-01225-01
	The state of the s	Clase de alerta	Fraude
	banco ripley	Tipo de incidente	Falsificación de Registros o Identidad
Bienvenido a	1	Nivel de riesgo	Alto
bancoripley.com	(-2150)	TLP	Blanco
	CSIRT	Fecha de lanzamiento original	22 de febrero de 2023
	Ingress a tu cuenta	Última revisión	22 de febrero de 2023
	RUT Ingresa tu RUT	Indicadores de compromiso	
0	Clave	URL sitio falso	
		https://bit[.]ly/3iHv9uH?l=www.ban	coripley.cl
	Ingresar	https://sam-tech[.]jp/bancoripley/cu	uenta-dusc/
	¿Olvidaste o se bioqueó tu clave?	https://web.bancoripley.cl.ngyokonu	utmarket[.]com/1677094832/login
		Dirección IP	
		[213.238.167.92]	
		Enlaces para revisar el informe:	
		https://www.csirt.gob.cl/alertas/8ffr	23-01225-01/
		https://www.csirt.gob.cl/media/202	3/02/8FFR23-01225-01.pdf



CSIRT advierte sitio falso que suplanta	a a Azaleia	
Alerta de seguridad cibernética	8FFR23-01226-01	
Clase de alerta	Fraude	
Tipo de incidente	Falsificación de Registros o Identidad	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	23 de febrero de 2023	
Última revisión	23 de febrero de 2023	
Indicadores de compromiso		
URL sitio falso		
https://azaleia.stdeck[.]com/		
Dirección IP		
[104.21.56.18]		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/alertas/8ffr23-01226-01/		
https://www.csirt.gob.cl/media/2023/02/8FFR23-01226-01.pdf		

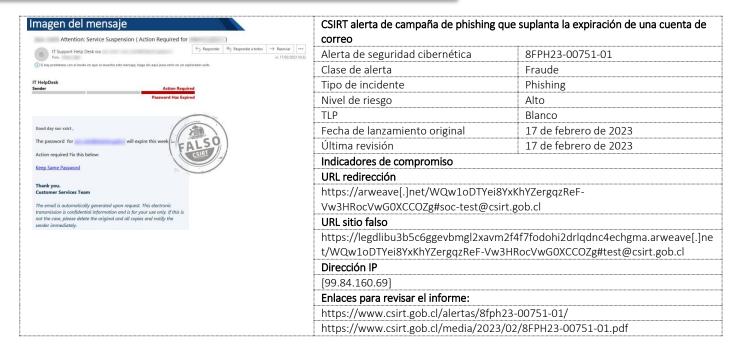


Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

2. Phishing



magen del mensaje		CSIRT alerta campaña de phishing que	e suplanta a Zimbra
Advertencia		Alerta de seguridad cibernética	8FPH23-00752-01
1. <am_ciudadmunicipal_spam@mdcc.gob.pe></am_ciudadmunicipal_spam@mdcc.gob.pe>	(Responder (Responder a todos → Reenviar (III) III . 20/02/2023 7:29	Clase de alerta	Fraude
contraseña expirará en 2 días para mantener su cuenta, amablemen a clic aquí y siga las instrucciones para retener su cuenta de correo		Tipo de incidente	Phishing
ficar la suscripción.		Nivel de riesgo	Alto
1:11	150	TLP	Blanco
	ALSO	Fecha de lanzamiento original	20 de febrero de 2023
		Última revisión	20 de febrero de 2023
h.		Indicadores de compromiso	
		URL sitio falso	
		https://diane-wight.mykajabi[.]com/	08jd
		Dirección IP	
		[104.18.19.84]	
		Enlaces para revisar el informe:	
		https://www.csirt.gob.cl/alertas/8fpl	h23-00752-01/
		https://www.csirt.gob.cl/media/2023	3/02/8FPH23-00752-01.pdf

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO



Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

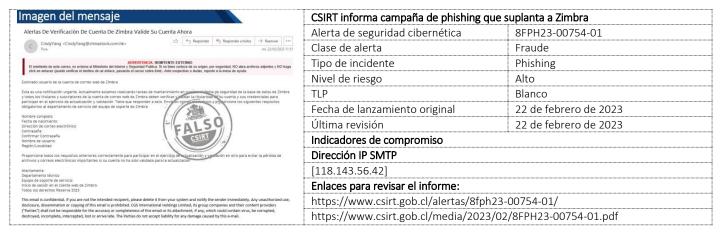
@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

Imagen del mensaje	CSIRT advierte campaña de phishing o	con falsa actualización de cuenta de correo
	Alerta de seguridad cibernética	8FPH23-00753-01
G Gob <capintos@sanidadpolicial.gl a="" p.uy="" responder="" th="" todos<="" w=""><td>Clase de alerta</td><td>Fraude</td></capintos@sanidadpolicial.gl>	Clase de alerta	Fraude
(-FNISO)	Tipo de incidente	Phishing
CSIRT	Nivel de riesgo	Alto
ACTUALIZA TU ACCESO	TLP	Blanco
Debido al mantenimiento reciente de la cuenta, debe actualizar su perfii para evitar limitaciones en su cuenta.	Fecha de lanzamiento original	22 de febrero de 2023
Actualizar ahora.	Última revisión	22 de febrero de 2023
PERSPECTIVE PRIVACY CONTACT US LOG IN	Indicadores de compromiso	
	URL sitio falso	
	https://heyflow[.]id/0onjd#start	
	Dirección IP	
	[216.239.34.21]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph	n23-00753-01/
	https://www.csirt.gob.cl/media/2023	3/02/8FPH23-00753-01.pdf

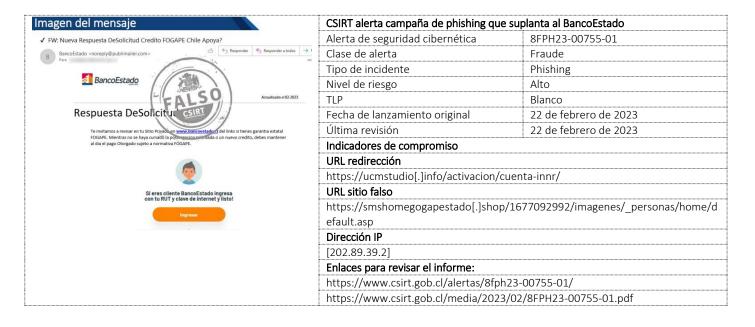


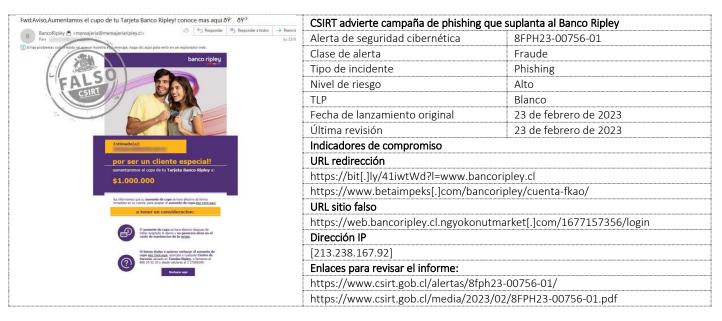


Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023





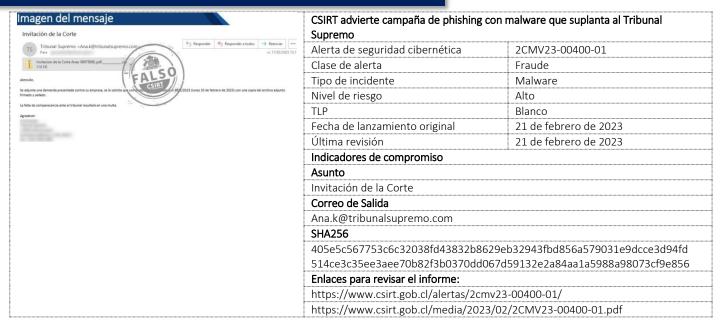


Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

3. Malware





Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

4. Vulnerabilidades



CSIRT comparte vulnerabilidad y mitig	CSIRT comparte vulnerabilidad y mitigaciones en FortiWeb		
Alerta de seguridad cibernética	9VSA23-00790-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Crítico		
TLP	Blanco		
Fecha de lanzamiento original	17 de febrero de 2023		
Última revisión	17 de febrero de 2023		
CVE			
CVE-2023-23777			
Fabricante			
Fortinet Productos afectados Fortinet FortiWeb: 7.0.0 – 7.0.1, 6.4.0 – 6.4.2, 6.3.6 – 6.3.18 Enlaces para revisar el informe:			
		https://www.csirt.gob.cl/vulnerabilida	ades/9vsa23-00790-01/
		https://www.csirt.gob.cl/media/2023/02/9VSA23-00790-01.pdf	



CSIRT comparte vulnerabilidad en FortiWan			
Alerta de seguridad cibernética	9VSA23-00791-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Crítico		
TLP	Blanco		
Fecha de lanzamiento original	17 de febrero de 2023		
Última revisión	17 de febrero de 2023		
CVE			
CVE-2022-33869 Fabricante Fortinet Productos afectados FortiWAN: 4.0.0 – 4.5.9 Enlaces para revisar el informe: https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00791-01/			
		https://www.csirt.gob.cl/media/2023/02/9VSA23-00791-01-1.pdf	

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO



Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023



	CSIRT comparte vulnerabilidades y mit	tigaciones en FortiWeb
	Alerta de seguridad cibernética	9VSA23-00792-01
	Clase de alerta	Vulnerabilidad
	Tipo de incidente	Sistema y/o Software Abierto
	Nivel de riesgo	Crítico
ļ	TLP	Blanco
	Fecha de lanzamiento original	20 de febrero de 2023
	Última revisión	20 de febrero de 2023
	CVE	
	CVE-2021-42756	
	Fabricantes	
	Fortinet Productos afectados FortiWeb versiones 5.x todas las versiones, versiones 6.0.7 e inferiores, versiones 6.1.2 e inferiores, versiones 6.2.6 e inferiores, versiones 6.3.16 e inferiores y versiones 6.4 todas las versiones.	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00792-01/	

https://www.csirt.gob.cl/media/2023/02/9VSA23-00792-01.pdf



	CSIRT comparte vulnerabilidad crítica e	n FortiNAC	
	Alerta de seguridad cibernética	9VSA23-00793-01	
	Clase de alerta	Vulnerabilidad	
	Tipo de incidente	Sistema y/o Software Abierto	
	Nivel de riesgo	Crítico	
1	TLP	Blanco	
Ţ	Fecha de lanzamiento original	20 de febrero de 2023	
	Última revisión	20 de febrero de 2023	
	CVE		
. >	CVE-2022-39952		
	Fabricante		
0	Fortinet		
	Productos afectados		
	FortiNAC versión 9.4.0		
	FortiNAC versión 9.2.0 a 9.2.5		
	FortiNAC versión 9.1.0 a 9.1.7		
	FortiNAC 8.8 todas las versiones		
	FortiNAC 8.7 todas las versiones		
	FortiNAC 8.6 todas las versiones		
	FortiNAC 8.5 todas las versiones		
FortiNAC 8.3 todas las versiones			
	Enlaces para revisar el informe:		
	https://www.csirt.gob.cl/vulnerabilidad	des/9vsa23-00793-01/	
	https://www.csirt.gob.cl/media/2023/0	02/9VSA23-00793-01.pdf	

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562)

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023



SIRT comparte vulnerabilidad en For	tiOS y FortiAuthenticator	
Alerta de seguridad cibernética	9VSA23-00794-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	22 de febrero de 2023	
Última revisión	22 de febrero de 2023	
CVE		
CVE-2022-22302		
Fabricante		
Fortinet		
Productos afectados		
FortiOS versión 6.4.0 a 6.4.1		
FortiOS versión 6.2.0 a 6.2.9		
FortiOS versión 6.0.0 a 6.0.13		
FortiAuthenticator versión 6.1.0		
FortiAuthenticator versión 6.0.0 a 6.0	0.4	
FortiAuthenticator 5.5 todas las versi	ones	
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-0079-01/		

https://www.csirt.gob.cl/media/2023/02/9VSA23-00794-01-1.pdf



CSIRT comparte vulnerabilidades en VMware Carbon Black App Control					
Alerta de seguridad cibernética	9VSA23-00795-01				
Clase de alerta	Vulnerabilidad				
Tipo de incidente	Sistema y/o Software Abierto				
Nivel de riesgo	Crítico				
TLP	Blanco				
Fecha de lanzamiento original	22 de febrero de 2023				
Última revisión	22 de febrero de 2023				
CVE					
CVE-2023-20858					
Fabricante VMware Productos afectados					
			ClamAV versiones 1.0.0 y anteriores; 0.105.1 y anteriores; y 0.103.7 y anteriores		
			Enlaces para revisar el informe: https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00795-01/ https://www.csirt.gob.cl/media/2023/02/9VSA23-00795-01.pdf		

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO



Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023



CSIRT comparte actualización de vulnerabilidad en la biblioteca de escaneo de terceros ClamAV de Cisco		
Alerta de seguridad cibernética	9VSA23-00789-02	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	16 de febrero de 2023	
Última revisión	23 de febrero de 2023	
CVE		
CVE-2023-20032		
CVE-2023-20052		
Fabricante		
Cisco Productos afectados ClamAV versiones 1.0.0 y anteriores; 0.105.1 y anteriores; y 0.103.7 y anteriores		

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00789-02/ https://www.csirt.gob.cl/media/2023/02/9VSA23-00789-02.pdf



<u> </u>	CSIRT comparte vulnerabilidad en FortiAnalyzer					
S S S S S S S S S S S S S S S S S S S	Alerta de seguridad cibernética	9VSA23-00796-01				
	Clase de alerta	Vulnerabilidad				
	Tipo de incidente	Sistema y/o Software Abierto				
Ĭ	Nivel de riesgo	Crítico				
ļ	TLP	Blanco				
	Fecha de lanzamiento original	23 de febrero de 2023				
9	Última revisión	23 de febrero de 2023				
CVE						
Fabricante Fortinet Productos afectados FortiAnalyzer versión 7.2.0 a 7.2.1. FortiAnalyzer versión 7.0.0 a 7.0.4 FortiAnalyzer versión 6.4.0 a 6.4.8						
				FortiAnalyzer versión 6.2.0 a 6.2.9		
				FortiAnalyzer versión 6.0.0 a 6.0.11		
				Enlaces para revisar el informe:		
				https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00796-01/		
				https://www.csirt.gob.cl/media/2023/0)2/9VSA23-00796-01.pdf	



Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

5. Noticias

Alerta de Seguridad | IoC´s de distintas amenazas cibernéticas

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, comparte algunos indicadores de compromisos de fuentes abiertas, nacionales e internacionales, de dos amenazas detectadas recientemente en nuestro país.

Una de ellas es una campaña de ransomware identificada como BlackCat, un conocido ransomware de servicio (Ransonware-as-a-Service), que aprovecha las credenciales de usuarios comprometidas para tener acceso a los sistemas.



Los vectores de entrada de esta amenaza pueden ser diversos, como las vulnerabilidades en las plataformas expuestas a internet, técnicas de ingeniería social, entre otros. Su objetivo principal es obtener acceso al Active Directory donde genera políticas de grupo (GPO) para la implementación de ransomware, aprovechando scripts de PowerShell, herramientas administrativas de Windows y Microsoft Sysinternals.

Sugerimos a las organizaciones, especialmente a la Red de Conectividad del Estado, evaluar la aplicación de cuarentenas sobre estos IoC, revisar el tráfico desde y fuera de su red.

IoC ransomware

Direcciones IP C2

89.44.9.243

142.234.157.246

45.134.20.66

146.0.77.15

37.120.238.58

185.220.102.253

152.89.247.207

198.144.121.93

94.232.41.155

89.163.252.230

45.153.160.140

23.106.223.97

139.60.161.161

Ver másí: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-iocs-amenazas-ciberneticas/

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

ttps://www.csirt.gob.cl

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgot

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

6. Concientización

Ciberconsejos para comprar seguros por internet

A la hora de comprar por Internet, ten cuidado con los vendedores falsos, quienes buscan robar dinero con ofertas o productos falsos. Para no caer en una estafa, te invitamos a leer los ciberconsejos del CSIRT de Gobierno: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-compras-internet/









https://www.csirt.gob.cl
Teléfonos: 1510 | + (562)

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

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 que los sitios web a los que se ingrese sean los oficiales.



Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Ministerio del Interior y Seguridad Pública Gobierno de Chile



BOLETÍN 13BCS23-00199-01 | SEMANA DEL 17 AL 23 DE FEBRERO DE 2023

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.

- Mauricio Rojas
- Patricio Hernández
- Nicole Raveau
- Cristopher León
- Alba Aguirre
- Andrea Vera
- Felipe Cortés
- Héctor Vergara
- Javier Godoy
- Carlos Ramírez
- Andrea Méndez
- Yuliany Oliveira
- Natalia Arenas

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl

Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl

@csirtgob