CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 190

SEMANA DEL 17 AL 23 DE FEBRERO 2023

LA 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

CONTENIDO

1. Sitios fraudulentos 3
2. Phishing 10
3. Malware 13
4. Vulnerabilidades 14
5. Noticias 18
6. Concientización 19
7. Recomendaciones y buenas prácticas 20
8. Muro de la Fama 21

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

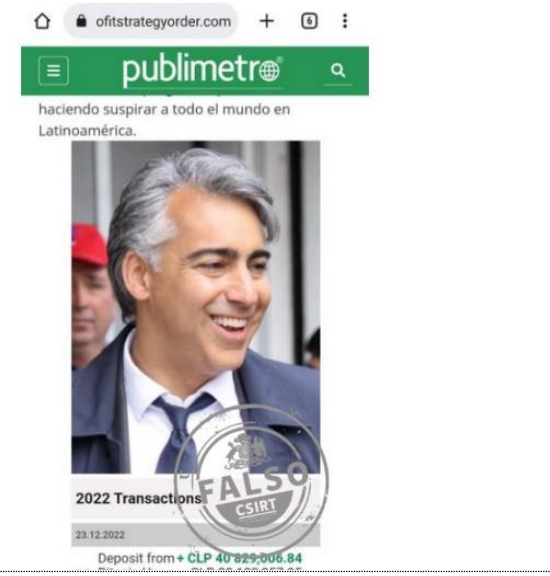
Imagen del sitio	CSIRT alerta sitio falso que suplanta a Publimetro	
	Alerta de seguridad cibernética	8FFR23-01213-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	17 de febrero de 2023
	Última revisión	17 de febrero de 2023
	Indicadores de compromiso	
	URL sitio falso	
	https://profitstrategyorder[.]com/	
	Dirección IP	
	[172.67.219.200]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr23-01213-01/	
	https://www.csirt.gob.cl/media/2023/02/8FFR23-01213-01.pdf	

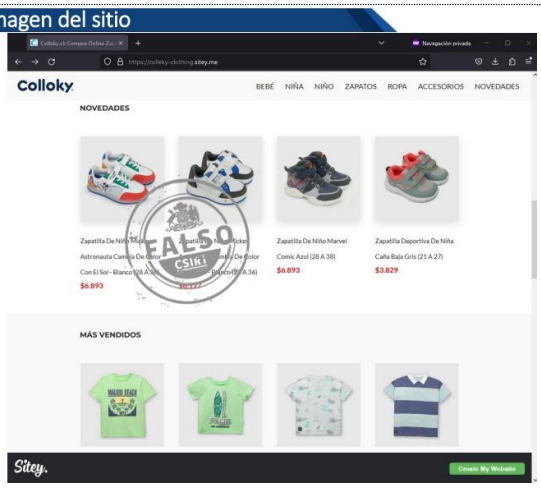
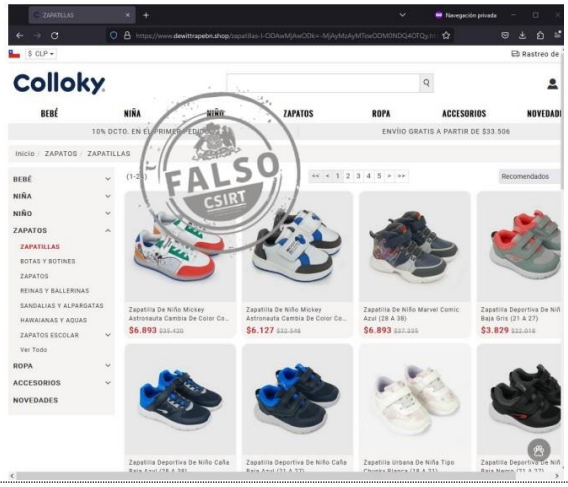
Imagen del sitio	CSIRT advierte sitio que suplanta a Colloky	
	Alerta de seguridad cibernética	8FFR23-01214-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	17 de febrero de 2023
	Última revisión	17 de 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/8ffr23-01214-01/	
	https://www.csirt.gob.cl/media/2023/02/8FFR23-01214-01-1.pdf	

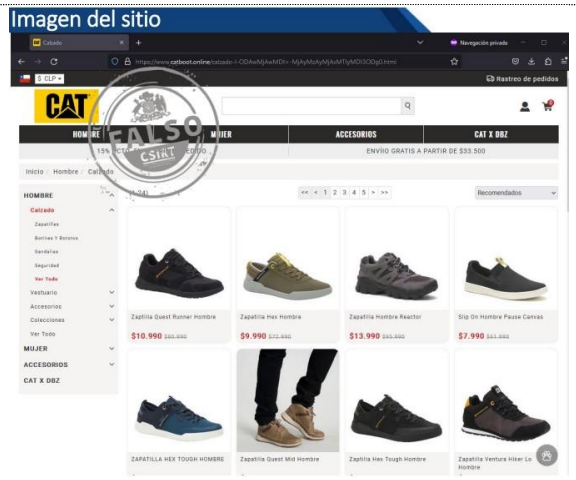
Imagen del sitio



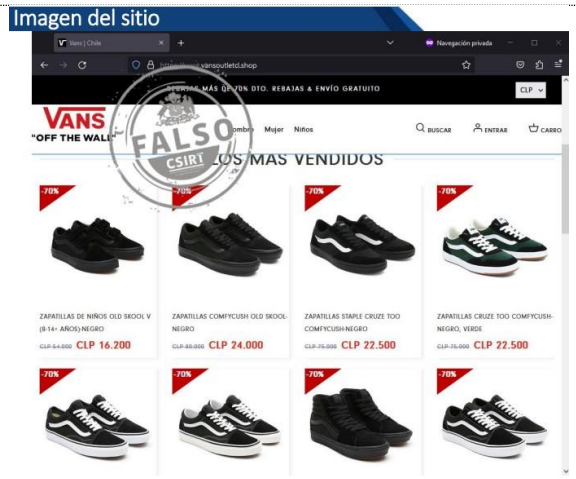
CSIRT advierte sitio web que suplanta a Colloky	
Alerta de seguridad cibernética	8FFR23-01215-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2023
Última revisión	17 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.dewittrapebn[.]shop/	
Dirección IP	
[167.160.3.16]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01215-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01215-01-1.pdf	

Imagen del sitio

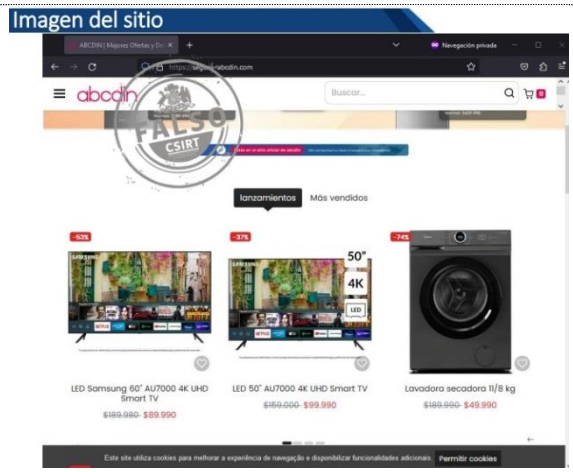
CSIRT alerta página web que suplanta a Colloky	
Alerta de seguridad cibernética	8FFR23-01216-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de febrero de 2023
Última revisión	17 de febrero de 2023
Indicadores 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/8ffr23-01216-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01216-01.pdf	



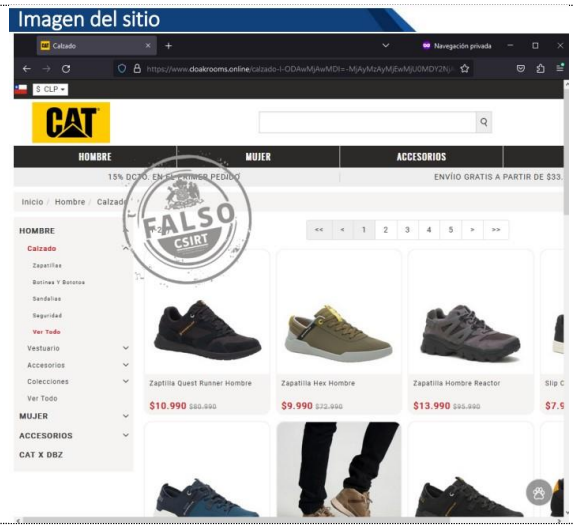
CSIRT advierte sitio que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01217-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de febrero de 2023
Última revisión	20 de febrero de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.catboot[.]online/	
Dirección IP	
[107.150.173.211]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01217-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01217-01.pdf	



CSIRT alerta de página web que suplanta 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	

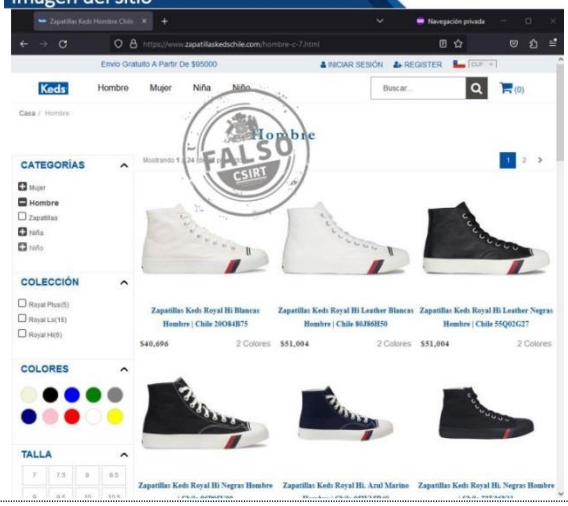


CSIRT alerta sitio web falso de ABCDIN	
Alerta de seguridad cibernética	8FFR23-01219-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de febrero de 2023
Última revisión	20 de febrero de 2023
Indicadores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



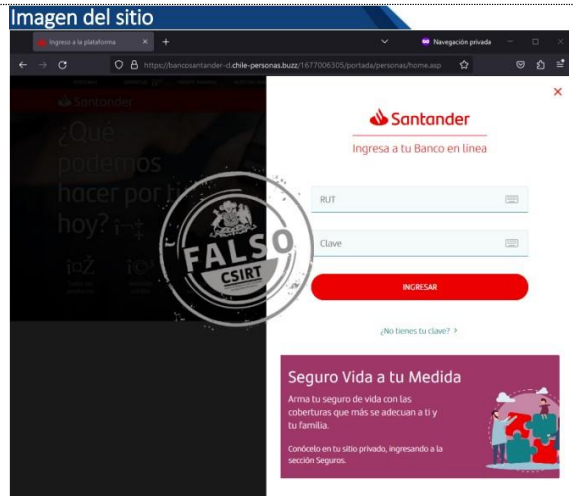
CSIRT advierte página web que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01220-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2023
Última revisión	21 de febrero de 2023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

Imagen del sitio



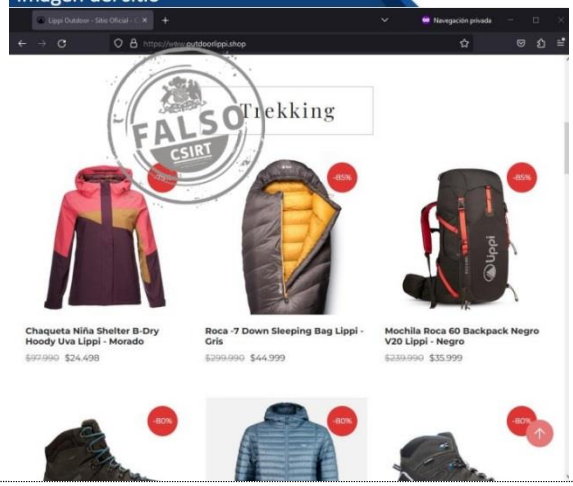
CSIRT alerta de sitio web falso de Keds	
Alerta de seguridad cibernética	8FFR23-01221-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2023
Última revisión	21 de febrero de 2023
Indicadores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

Imagen del sitio



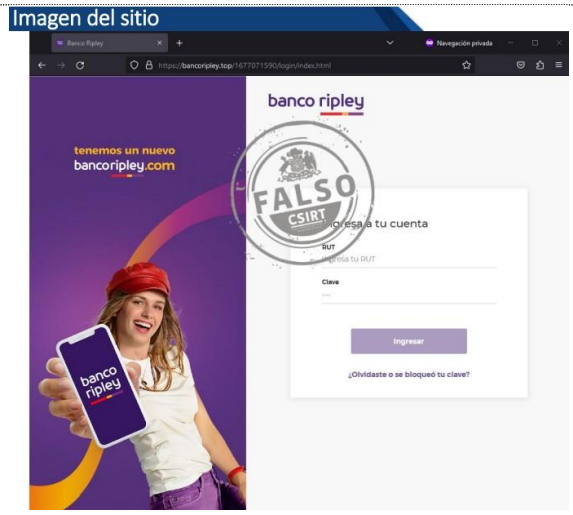
CSIRT informa de página web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR23-01222-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2023
Última revisión	22 de febrero de 2023
Indicadores de compromiso	
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:	
https://www.csirt.gob.cl/alertas/8ffr23-01222-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01222-01.pdf	

Imagen del sitio



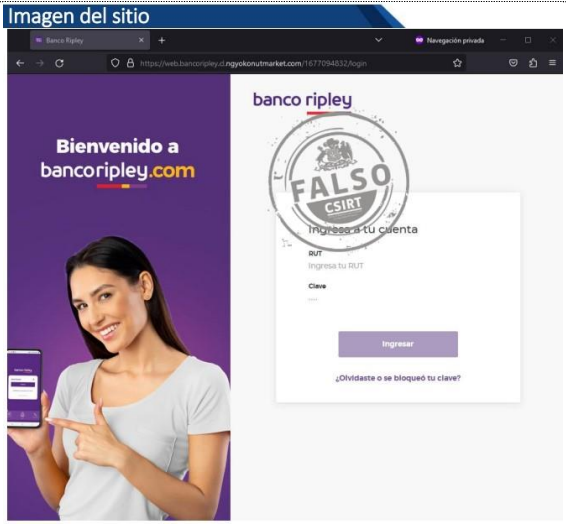
CSIRT advierte sitio web falso de Lippi	
Alerta de seguridad cibernética	8FFR23-01223-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2023
Última revisión	22 de febrero de 2023
Indicadores 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	

Imagen del sitio



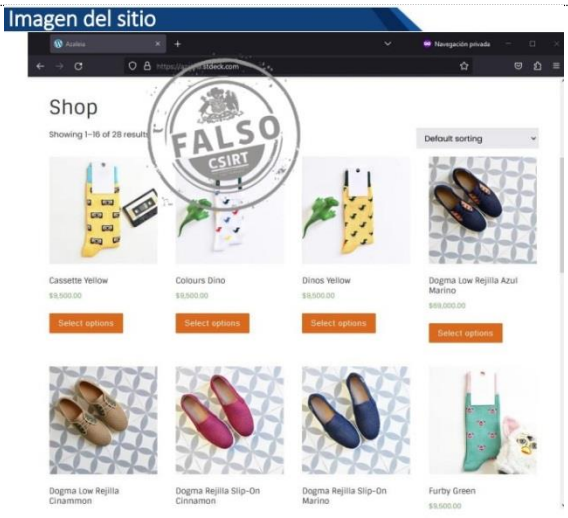
CSIRT alerta página web falsa que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01224-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2023
Última revisión	22 de febrero 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	

Imagen del sitio



CSIRT advierte sitio falso que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01225-01
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://bit[.]ly/3iHv9uH?l=www.bancoripley.cl	
https://sam-tech[.]jp/bancoripley/cuenta-dusc/	
https://web.bancoripley.cl.ngyokonutmarket[.]com/1677094832/login	
Dirección IP	
[213.238.167.92]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01225-01/	
https://www.csirt.gob.cl/media/2023/02/8FFR23-01225-01.pdf	

Imagen del sitio



CSIRT advierte sitio falso que suplanta 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	

2. Phishing

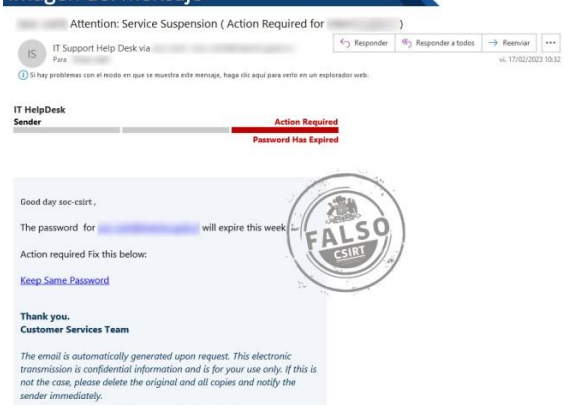
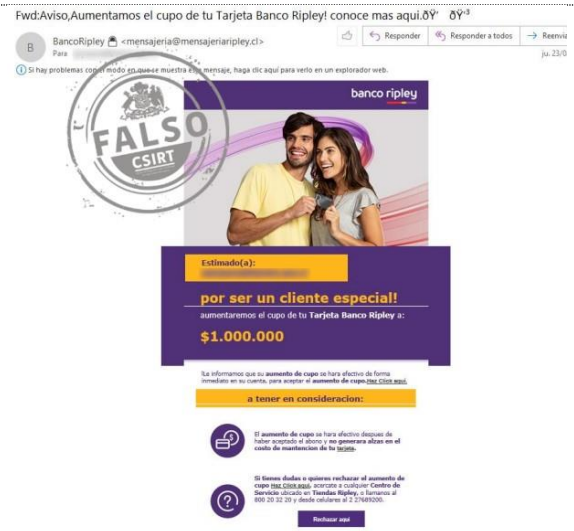
Imagen del mensaje		
	**CSIRT alerta de campaña de phishing que suplanta la expiración de una cuenta de correo**	
	Alerta de seguridad cibernética	8FPH23-00751-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	17 de febrero de 2023
	Última revisión	17 de febrero de 2023
	Indicadores de compromiso	
	URL redirección	
	https://arweave[.]net/WQw1oDTYei8YxKhYZergqzReF-Vw3HRocVwG0XCCOZg#soc-test@csirt.gob.cl	
	URL sitio falso	
	https://legdlibu3b5c6ggevbmgl2xavm2f4f7fodohi2drlqdnc4echgma.arweave[.]net/WQw1oDTYei8YxKhYZergqzReF-Vw3HRocVwG0XCCOZg#test@csirt.gob.cl	
	Dirección IP	
	[99.84.160.69]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00751-01/	
	https://www.csirt.gob.cl/media/2023/02/8FPH23-00751-01.pdf	

Imagen del mensaje		
	**CSIRT alerta campaña de phishing que suplanta a Zimbra**	
	Alerta de seguridad cibernética	8FPH23-00752-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	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://diane-wight.mykajabi[.]com/08jd	
	Dirección IP	
	[104.18.19.84]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph23-00752-01/	
	https://www.csirt.gob.cl/media/2023/02/8FPH23-00752-01.pdf	

Imagen del mensaje	
	
CSIRT advierte campaña de phishing con falsa actualización de cuenta de correo	
Alerta de seguridad cibernética	8FPH23-00753-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
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://heyflow[.]id/0onjd#start	
Dirección IP	
[216.239.34.21]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00753-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00753-01.pdf	

Imagen del mensaje	
	
CSIRT informa campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH23-00754-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
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	
Dirección IP SMTP	
[118.143.56.42]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00754-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00754-01.pdf	

CSIRT alerta campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00755-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
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 redirección	
https://ucmstudio[.]info/activacion/cuenta-innr/	
URL sitio falso	
https://smshomegogapestado[.]shop/1677092992/imagenes/_personas/home/default.asp	
Dirección IP	
[202.89.39.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00755-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00755-01.pdf	



CSIRT advierte campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00756-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
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 redirección	
https://bit[.]ly/41iwtWd?l=www.bancoripley.cl	
https://www.betaimpeks[.]com/bancoripley/cuenta-fkao/	
URL sitio falso	
https://web.bancoripley.cl.ngyokonutmarket[.]com/1677157356/login	
Dirección IP	
[213.238.167.92]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00756-01/	
https://www.csirt.gob.cl/media/2023/02/8FPH23-00756-01.pdf	

3. Malware

Imagen del mensaje	CSIRT advierte campaña de phishing con malware que suplanta al Tribunal Supremo	
	Alerta de seguridad cibernética	2CMV23-00400-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	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	
	Asunto	
	Invitación de la Corte	
	Correo de Salida	
	Ana.k@tribunalsupremo.com	
	SHA256	
	405e5c567753c6c32038fd43832b8629eb32943fbd856a579031e9dcce3d94fd 514ce3c35ee3aee70b82f3b0370dd067d59132e2a84aa1a5988a98073cf9e856	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv23-00400-01/	
	https://www.csirt.gob.cl/media/2023/02/2CMV23-00400-01.pdf	

4. Vulnerabilidades

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/vulnerabilidades/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	

CSIRT comparte vulnerabilidades y mitigaciones 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
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 en FortiNAC	
Alerta de seguridad cibernética	9VSA23-00793-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de febrero de 2023
Última revisión	20 de febrero de 2023
CVE	
CVE-2022-39952	
Fabricante	
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/vulnerabilidades/9vsa23-00793-01/	
https://www.csirt.gob.cl/media/2023/02/9VSA23-00793-01.pdf	

CSIRT comparte vulnerabilidad en FortiOS 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 6.0.4 FortiAuthenticator 5.5 todas las versiones	
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	

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	

CSIRT comparte vulnerabilidad en FortiAnalyzer	
Alerta de seguridad cibernética	9VSA23-00796-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	23 de febrero de 2023
Última revisión	23 de febrero de 2023
CVE	
CVE-2022-30304	
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/2023/02/9VSA23-00796-01.pdf	

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

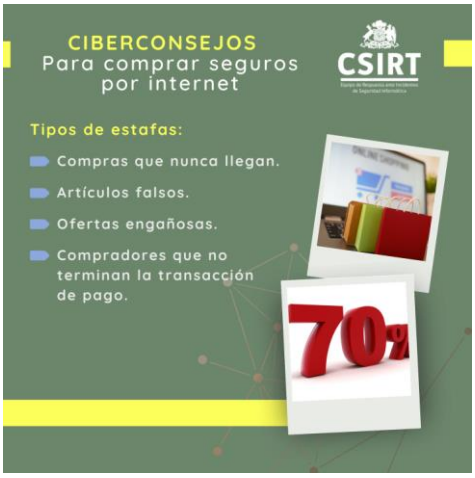
89.44.9.243
142.234.157.246
45.134.20.66
146.0.77.15
37.120.238.58
185.220.102.253
152.89.247.207
198.144.121.93
94.232.41.155
89.163.252.230
45.153.160.140
23.106.223.97
139.60.161.161

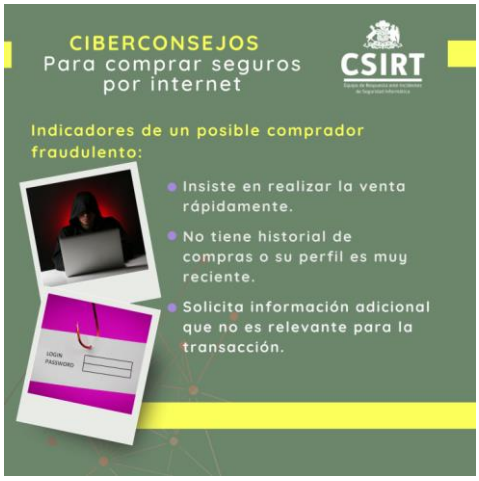
Ver másí: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-iocs-amenazas-ciberneticas/

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/





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.

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.24 13:55:51 -03'00'