CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 181

SEMANA DEL 16 AL 22 DE DICIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

24

Las mitigaciones son útiles en productos de Fortinet y Atlassian.

IP INFORMADAS

24

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

URL ADVERTIDAS

25

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

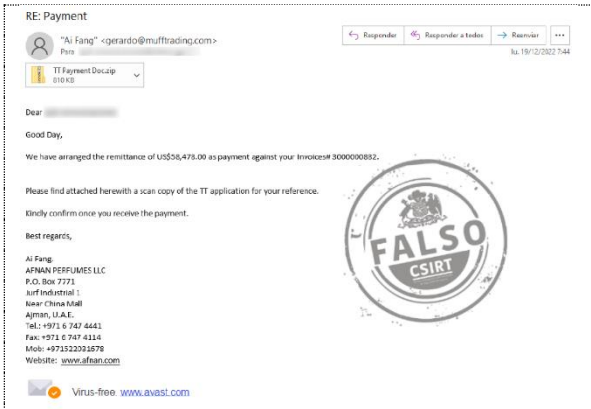
3

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 campaña de phishing con malware, que suplanta a Muff Trading	
Alerta de seguridad cibernética	2CMV22-00394-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
Asunto	
RE: Payment	
Correo de salida	
gerardo@mufftrading[.]com	
SHA256	
b375ace043904ca1884316d38124698993ffb28ed27cae8deb3559867d16e7cb 589c67cd28abd40173abc9bfe2fb2b80eaa905bc8bd0be9b70d04c73829a7423 TT 589c67cd28abd40173abc9bfe2fb2b80eaa905bc8bd0be9b70d04c73829a7423	
URL	
mail.sseximclearing[.]com:587	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00394-01/	
https://www.csirt.gob.cl/media/2022/12/2CMV22-00394-01.pdf	

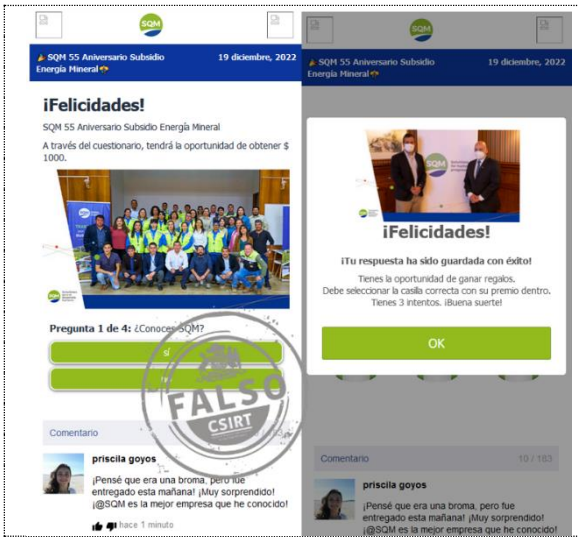
2. Ataques de fuerza bruta

CSIRT alerta de ataques de fuerza bruta contra el protocolo SMTP	
Alerta de seguridad cibernética	4IIV22-00058-01
Clase de alerta	Intento de intrusión
Tipo de incidente	Intento de intrusión – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022
Indicadores de compromiso	
Direcciones IP	
[80.94.95.206] [103.74.103.3] [192.227.217.208] [141.98.10.236] [103.153.78.188] [176.111.173.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iiv22-00058-01/	
https://www.csirt.gob.cl/media/2022/12/4IIV22-00058-01.pdf	

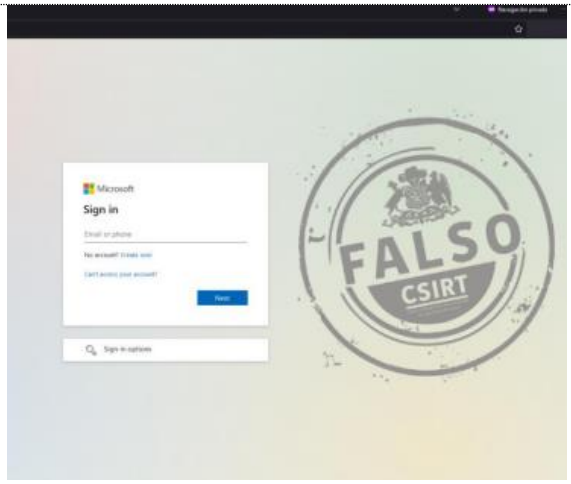
3. Sitios fraudulentos

CSIRT alerta de una página fraudulenta que suplanta a Fonasa	
Alerta de seguridad cibernética	8FFR22-01163-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2022
Última revisión	7 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//analystrefuse[.]top/2s4UrH3C/fonasaw/?_t=1671133961633#1671134157104	
Dirección IP	
[172.67.188.84]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01163-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01163-01.pdf	

CSIRT alerta de una página fraudulenta que suplanta al Jumbo	
Alerta de seguridad cibernética	8FFR22-01164-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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	
URL sitio falso	
https[:]//analystrefuse[.]top/WD5O9nYJ/jumbo-Christmas/?_t=1671135090835#1671135091839	
Dirección IP	
[172.67.188.84]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01164-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01164-01.pdf	

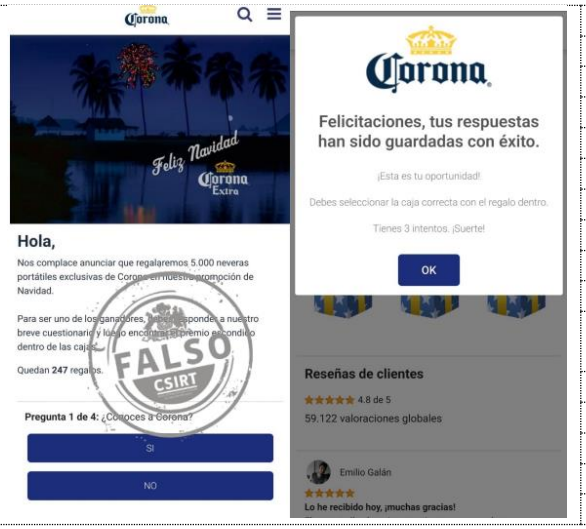


CSIRT alerta de página fraudulenta que suplanta a SQM	
Alerta de seguridad cibernética	8FFR22-01165-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//bpathd[.]cyou/H7t7E3fG/sqmw/?_t=1671452098934#1671452102428	
Dirección IP	
[172.67.219.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01165-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01165-01.pdf	

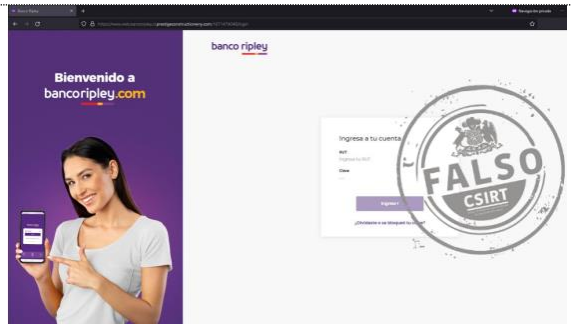


CSIRT alerta por página fraudulenta que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01166-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//sjcsbm[.]ru/ID-63a05f04b8fda	
Dirección IP	
[172.67.219.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01166-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01166-01.pdf	

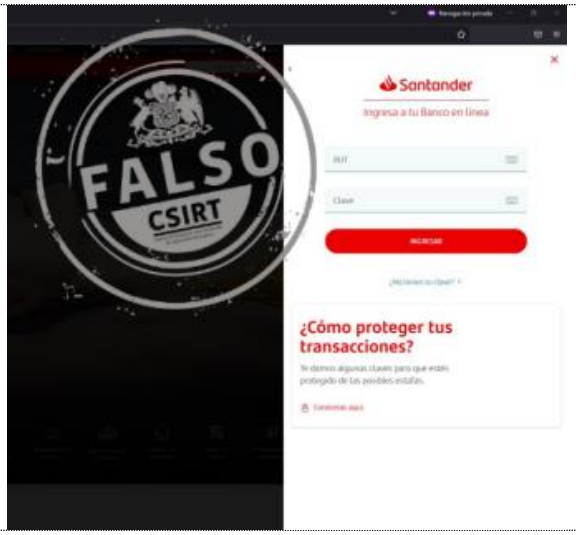
CSIRT alerta de una página fraudulenta que suplanta a Adobe Acrobat	
Alerta de seguridad cibernética	8FFR22-01167-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//www.patagonia-nuestra[.]cl/invioces/inv/index.php	
Dirección IP	
[186.64.116.35]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01167-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01167-01.pdf	



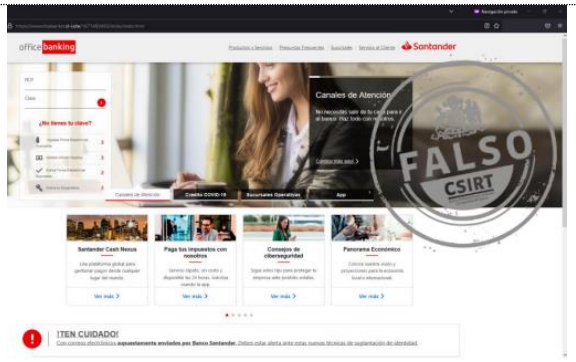
CSIRT alerta de una página fraudulenta que suplanta a cerveza Corona	
Alerta de seguridad cibernética	8FFR22-01168-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//tinyurl4[.]ru/BRuwjlMy/ https[:]//tinyurl4[.]ru/BRuwjlMy/#1671463113414	
Dirección IP	
[104.21.84.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01168-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01168-01.pdf	



CSIRT alerta de página fraudulenta que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR22-01169-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//www.web.bancoripley.cl.prestigeconstructionwny[.]com/1671474048/login	
Dirección IP	
[192.185.21.172]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01169-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01169-01.pdf	

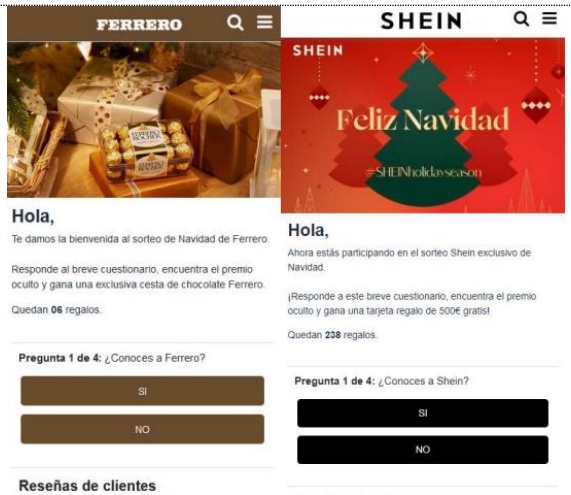


CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01170-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//brancosantander-cl.clavecl[.]top/1671474365/portada/personas/home.asp	
Dirección IP	
[104.21.17.124]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01170-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01170-01.pdf	

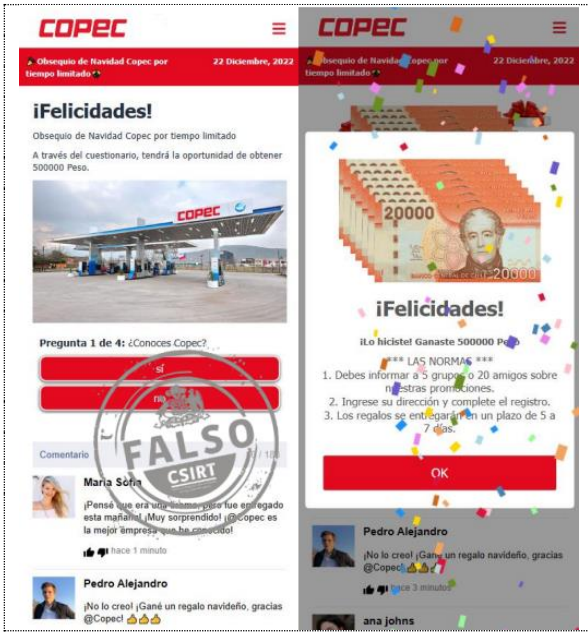


CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01171-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//wwwoficebankin.cl-l[.]site/1671478897/inicio/index.html	
Dirección IP	
[104.21.55.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01171-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01171-01.pdf	

CSIRT alerta ante sitio fraudulento que suplanta a cerveza Corona	
Alerta de seguridad cibernética	8FFR22-01172-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//tinyurl4[.]ru/chrcorlat/#1671635678096	
Dirección IP	
[172.64.199.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01172-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01172-01.pdf	



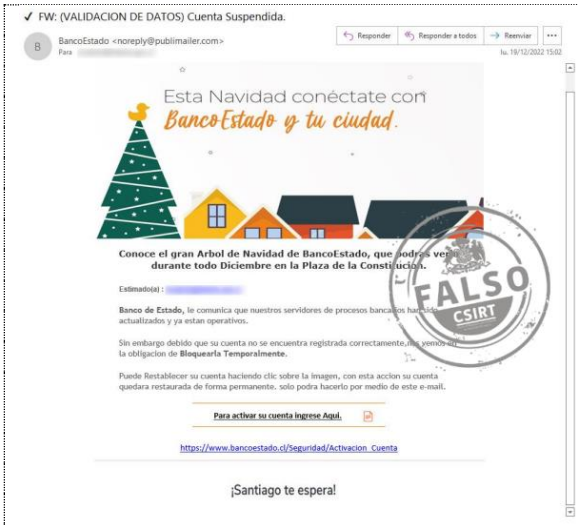
CSIRT alerta de 1.849 sitios fraudulentos que suplantan a populares marcas	
Alerta de seguridad cibernética	8FFR22-01173-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//tinyurl4[.]ru/	
Dirección IP	
[172.64.199.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01173-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01173-01.pdf	



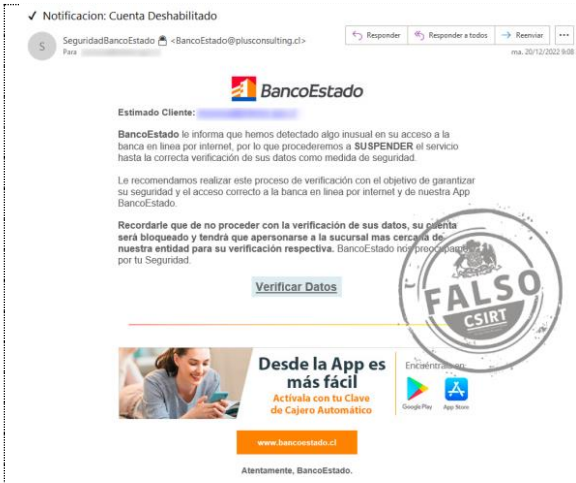
CSIRT alerta de una página fraudulenta que suplanta a Copec	
Alerta de seguridad cibernética	8FFR22-01174-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//widtco[.]cyou/IN8PHMDm/Copecwa/?_t=1671717370065#1671717897263	
Dirección IP	
[104.21.2.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01174-01/	
https://www.csirt.gob.cl/media/2022/12/8FFR22-01174-01.pdf	

4. Phishing

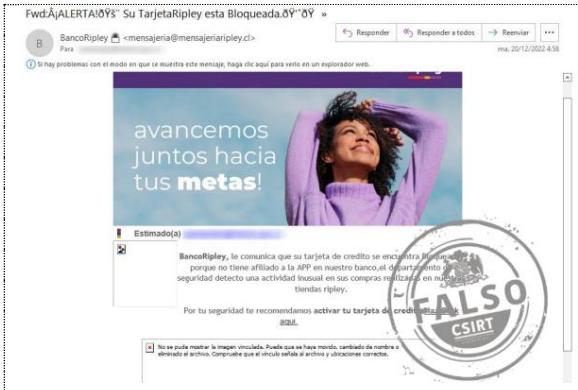
CSIRT alerta de campaña de phishing con sextorsión	
Alerta de seguridad cibernética	8FPH22-00681-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00681-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00681-01.pdf	



CSIRT alerta de campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH22-00682-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-aotq/	
URL sitio falso	
https[:]//newbailando[.]com/1671473291/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.7.84]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00682-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00682-01.pdf	



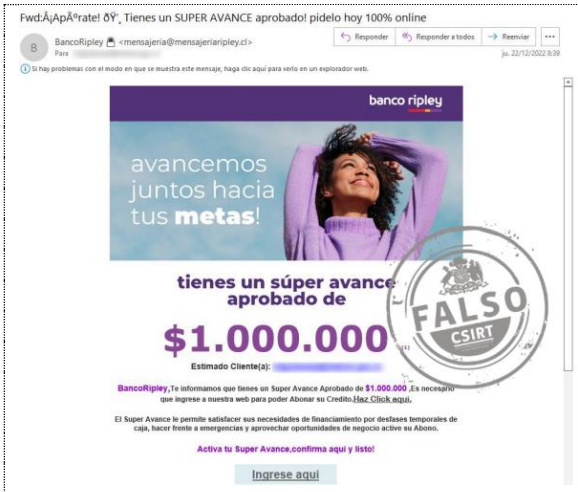
CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00683-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https[:]//avengerpati[.]com/activacion/cuenta-veqo/	
URL sitio falso	
https[:]//nmhpatito[.]info/1671548369/imagenes/_personas/home/default.asp	
Dirección IP	
[162.241.60.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00683-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00683-01.pdf	



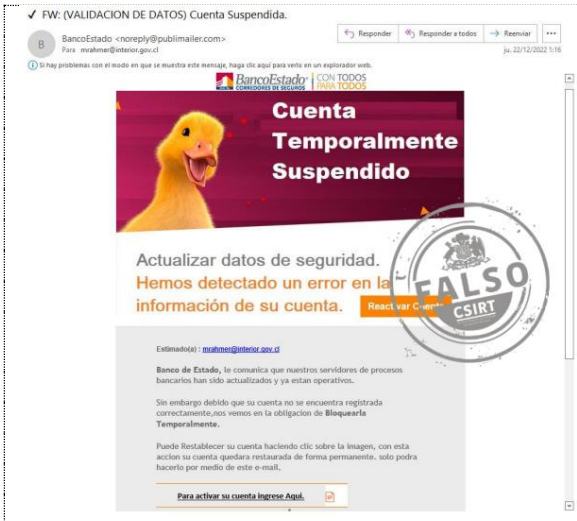
CSIRT alerta de campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00684-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3G5nHSG?l=www.bancoripley.cl https://worldwidefakenote[.]com/bancoripley/cuenta-jhcp/	
URL sitio falso	
https[:]//web-bancoripley-cl.wonthaggicaravans.com[.]au/1671549855/login	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00684-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00684-01.pdf	

CSIRT alerta de campaña de phishing por WhatsApp, que suplanta a Coca-Cola	
Alerta de seguridad cibernética	8FPH22-00685-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022
Indicadores de compromiso	
URL redirección	
https[:]//tinyurl4[.]ru/WuBGTYXv/	
Dirección IP	
[172.64.199.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00685-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00685-01.pdf	

CSIRT alerta ante campaña de phishing por Whatsapp que suplanta a Líder	
Alerta de seguridad cibernética	8FPH22-00686-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2022
Última revisión	21 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//lnkshort[.]ru/ETSBcxBs/#1671627265184	
Dirección IP	
[172.67.190.26]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00686-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00686-01.pdf	



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00687-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//web-bancoripley-cl.buckrealty[.]net/1671711266/login	
URL sitio redirección	
https[:]//bit[.]ly/3ChUzFR?l=www.bancoripley.cl https://web-bancoripley-cl.buckrealty[.]net/	
Dirección IP	
[64.91.247.208]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00687-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00687-01.pdf	



CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00688-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//newbailando[.]com/1671712402/imagenes/_personas/home/default.asp	
URL sitio redirección	
https[:]//ucmstudio.info/activacion/cuenta-aotq/	
Dirección IP	
[173.249.58.117]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00688-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00688-01.pdf	

5. Vulnerabilidades

CSIRT alerta de varias vulnerabilidades que afectan a diversos productos de VMware		
Alerta de seguridad cibernética	9VSA22-00756-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	19 de diciembre de 2022	
Última revisión	19 de diciembre de 2022	
CVE		
CVE-2021-39144	CVE-2022-31693	CVE-2022-31703
CVE-2022-31678	CVE-2022-31696	CVE-2022-31700
CVE-2022-31685	CVE-2022-31697	CVE-2022-31701
CVE-2022-31686	CVE-2022-31698	CVE-2022-31705
CVE-2022-31687	CVE-2022-31699	CVE-2022-31707
CVE-2022-31688	CVE-2022-31702	CVE-2022-31708
CVE-2022-31689		
Fabricantes		
VMware		
Productos afectados		
VMware Cloud Foundation VMware Workspace ONE Assist VMware Tools for Windows VMware ESXi and vCenter Server VMware vRealize Network Insight (vRNI) VMware Workspace ONE Access (Access) VMware Identity Manager (vIDM) VMware Cloud Foundation (Cloud Foundation)		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00756-01/		
https://www.csirt.gob.cl/media/2022/12/9VSA22-00756-01.pdf		

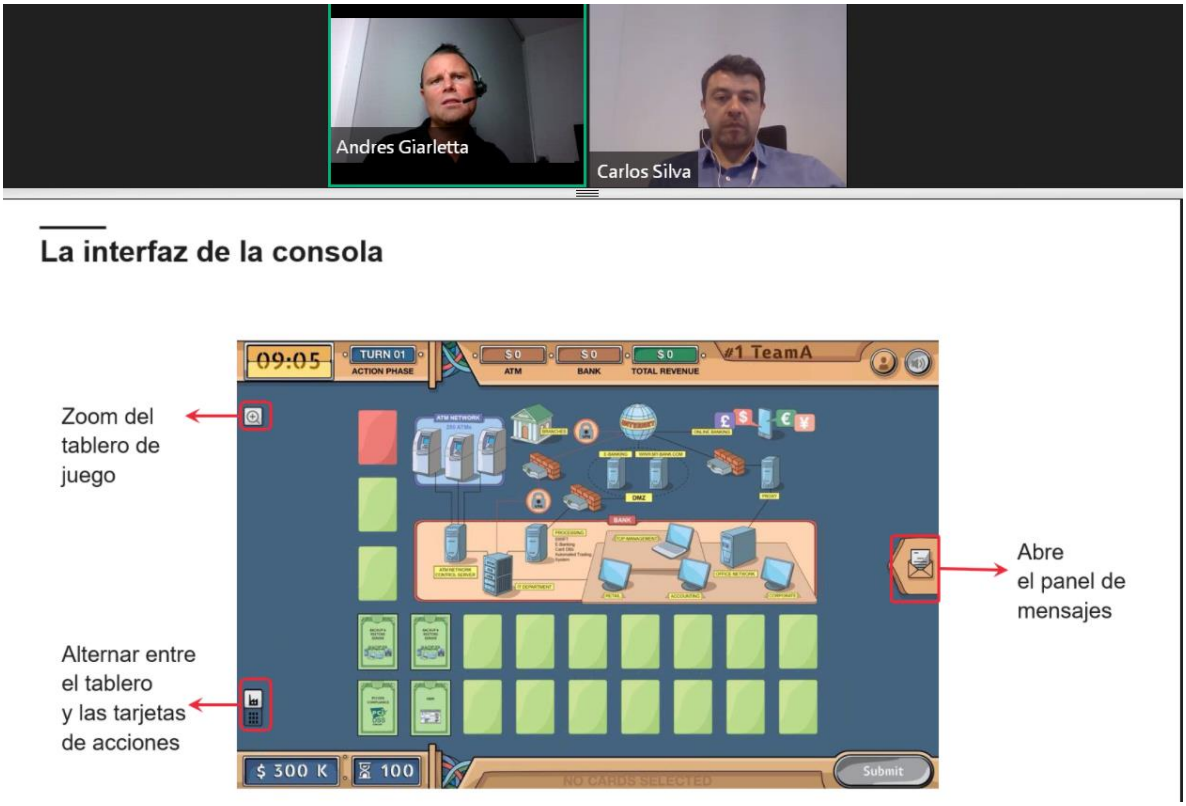
CSIRT alerta de vulnerabilidades que afectan a Samba	
Alerta de seguridad cibernética	9VSA22-00757-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022
CVE	
CVE-2022-38023	CVE-2022-37967
CVE-2022-37966	CVE-2022-45141
Fabricantes	
Samba	
Productos afectados	
Versiones de Samba anteriores a 4.17.4, 4.16.8 y 4.15.13.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00757-01/	

https://www.csirt.gob.cl/media/2022/12/9VSA22-00757-01.pdf	
CSIRT alerta de vulnerabilidad de riesgo medio en macOS	
Alerta de seguridad cibernética	9VSA22-00758-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022
CVE	
CVE-2022-42821	
Fabricantes	
Apple	
Productos afectados	
Versiones anteriores a macOS Monterey 12.6.2, macOS Big Sur 11.7.2 y macOS Ventura 13.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00758-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00758-01.pdf	

6. Actualidad

Simulación de entrenamiento para el Retail Financiero

El lunes 19 de diciembre, como parte del convenio que la Asociación del Retail Financiero suscribió con el CSIRT de Gobierno, más de 35 ejecutivos de las empresas que integran el comité de ciberseguridad de la Asociación, participaron en la Kaspersky Interactive Protection Simulation (KIPS). La instancia de capacitación consta de un juego de simulación virtual e interactivo desarrollado por Karspersky, instancia en que los participantes se enfrentaron a los ciberataques más comunes en Chile y Latinoamérica, debiendo tomar decisiones para contrarrestar sus efectos y resguardar la seguridad de la operación.



7. Concientización

Ciberconsejos para evitar caer en concursos falsos

Durante diciembre, y a días de la Navidad, este tipo de fraudes han comenzado a propagarse de forma más recurrente. Delincuentes difunden a través de WhatsApp o mensajes de texto un falso sorteo y solicitan difundir la falsa campaña entre sus amigos. Quienes hagan clic son redirigidas a sitios web maliciosos que solicitan sus datos de tarjeta de crédito. Además, existe la posibilidad que los delincuentes secuestren el WhatsApp de la víctima.

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-falsos-concursos/.

8. 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.

9. 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.

- David Soto
- Sebastián Muñoz
- Gonzalo Andrés Araya Navarrete
- Rodrigo Javier Machado Villegas
- Rodrigo Patricio Velásquez Córdoba
- Héctor Andrés Verdejo Morales
- Edison Rodríguez