CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 177

SEMANA DEL 18 AL 24 DE NOVIEMBRE

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

3

Las mitigaciones son útiles en productos de Fortinet y Atlassian.

IP INFORMADAS

25

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

URL ADVERTIDAS

32

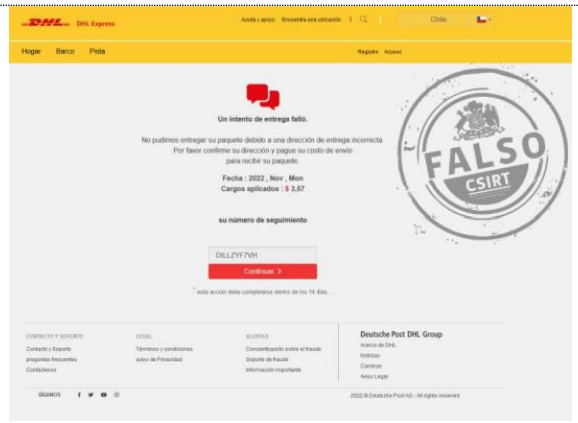
Asociadas a sitios fraudulentos y campañas de phishing y malware

CONTENIDO

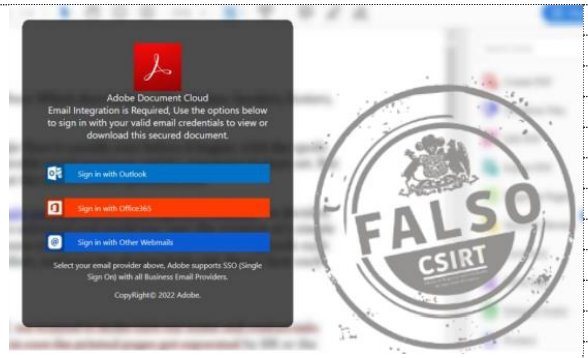
1. Sitios fraudulentos 3
2. Phishing 7
3. Ataques de Fuerza Bruta 12
4. Vulnerabilidades 13
5. Concientización 14
6. Recomendaciones y buenas prácticas 15
7. Muro de la Fama 16

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

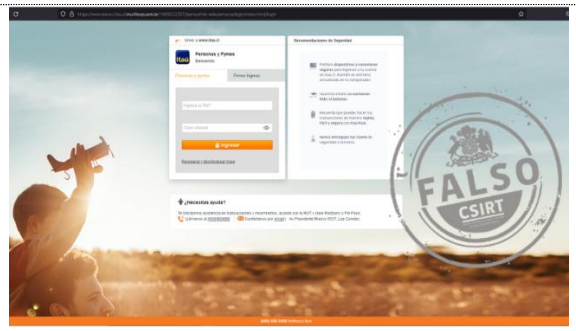
1. Sitios fraudulentos



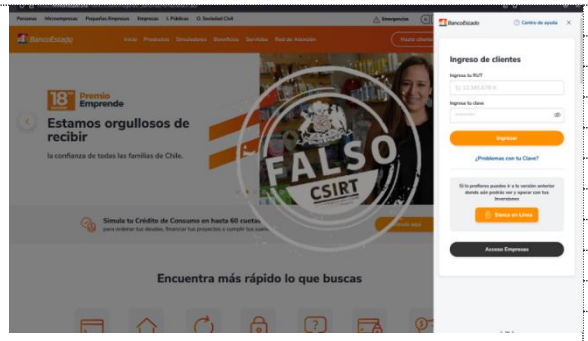
CSIRT advierte de sitio falso que suplanta a DHL	
Alerta de seguridad cibernética	8FFR22-01138-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2022
Última revisión	21 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://delhome.cabanashuaquen[.]cl/public/TGOdpFODBEq8a5UfYxUA6dbm4VpIUfff https://delhome.cabanashuaquen[.]cl/public/TGOdpFODBEq8a5UfYxUA6dbm4VpIUfff/payment?	
Dirección IP	
[186.64.118.55]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01138-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01138-01-1.pdf	



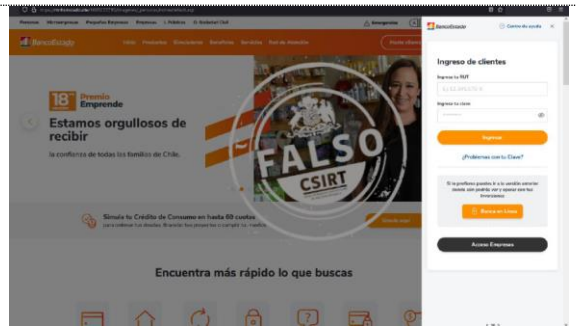
CSIRT alerta de página fraudulenta que suplanta a Adobe Acrobat	
Alerta de seguridad cibernética	8FFR22-01139-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://motoemotion{.}cl/wp-includes/js/tinymce/langs/htacces/os/	
Dirección IP	
[186.64.117.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01139-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01139-01.pdf	



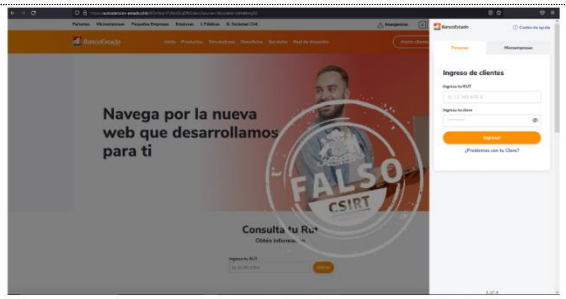
CSIRT alerta de página fraudulenta que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR22-01140-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.banco.itau.cl.murillovp.com[.]br/1669222357/bancochile-web/persona/login/index.html/login	
Dirección IP	
[162.241.203.61]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01140-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01140-01.pdf	



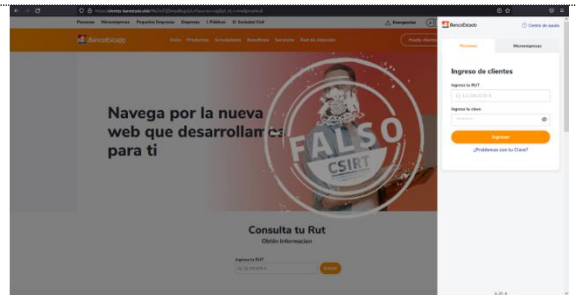
CSIRT alerta de nueva página que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01141-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://mnhsmstado[.]site/1669223117/imagenes/_personas/home/default.asp	
Dirección IP	
[47.87.139.183]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01141-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01141-01.pdf	



CSIRT alerta ante sitio falso que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01142-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://mnhsmstado[.]site/1669223117/imagenes/_personas/home/default.asp	
Dirección IP	
[47.87.139.183]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01142-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01142-01.pdf	



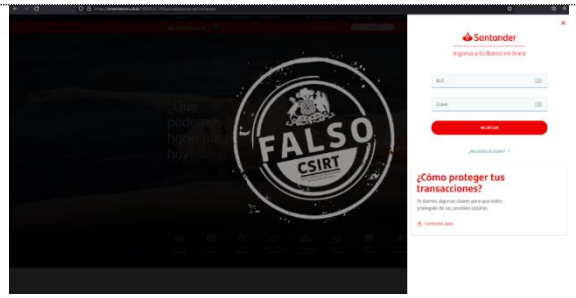
CSIRT alerta ante web fraudulenta que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01143-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://autoatencion-estado{.}click/AOvVaw1FcNbz0LaDfbS/esrc?source=t&nodeId=jd4eblmg53	
Dirección IP	
[104.21.86.191]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01143-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01143-01.pdf	



CSIRT alerta de sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR22-01144-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://clientes-banestado.click/WqTvcFQDmpdBcgzG/url?source=usg&pf_rd_r=4ndfjpmphkc6	
Dirección IP	
[104.21.56.178]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01144-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01144-01.pdf	

CSIRT alerta de página fraudulenta que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR22-01145-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://cuotas-creditos.web[.]app/inicio/banca	
Dirección IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01145-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01145-01.pdf	

CSIRT alerta ante web fraudulenta que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR22-01146-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://cuotas-creditos.firebaseapp[.]com/inicio/banca	
Dirección IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01146-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01146-01.pdf	

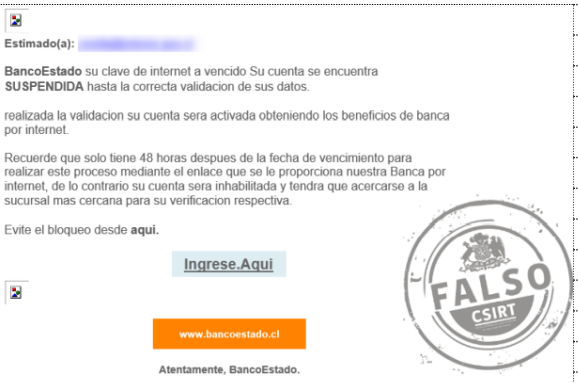


CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01147-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de noviembre de 2022
Última revisión	23 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://nostracontrical[.]com/cuentas/cuenta-test/ https://crownverano[.]club/1669232169/portada/personas/home.asp	
Dirección IP	
[162.241.60.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01147-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01147-01.pdf	

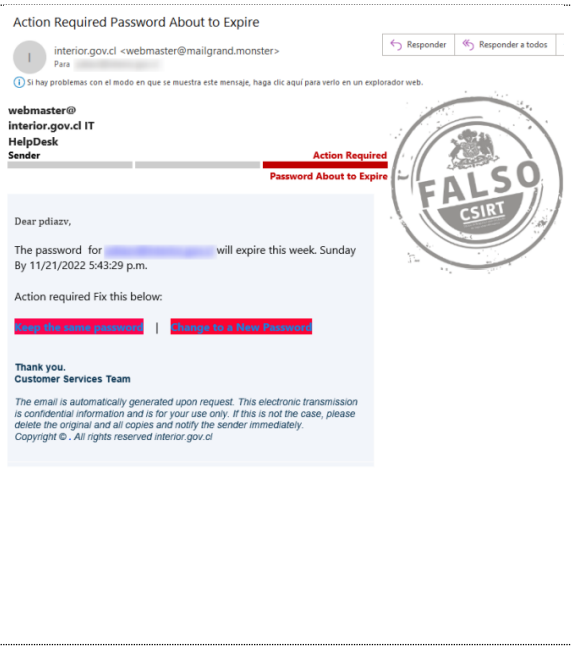
2. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00652-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de noviembre de 2022
Última revisión	18 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://razapotenew[.]com/activacion/cuenta-fctb/	
URL sitio falso	
https://rotafonorpp[.]com/1668778297/imagenes/_personas/home/default.asp	
Dirección IP	
[190.107.176.120]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00652-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00652-01.pdf	

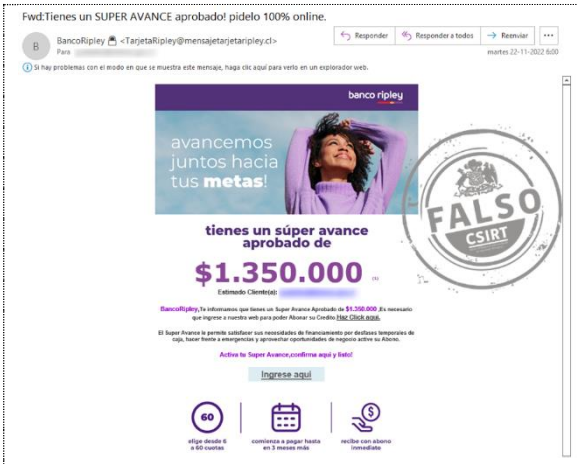
CSIRT alerta de web fraudulenta que suplanta login de Zimbra	
Alerta de seguridad cibernética	8FPH22-00653-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de noviembre de 2022
Última revisión	18 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://firebasestorage[.]googleapis.com/v0/b/tex778966.appspot.com/o/index.html?alt=media&token=03b0ea44-5387-4985-ac5c-d90a3a4d0e1a	
URL sitio falso	
https://firebasestorage[.]googleapis.com/v0/b/tex778966.appspot.com/o/index.html?alt=media&token=03b0ea44-5387-4985-ac5c-d90a3a4d0e1a	
Dirección IP	
[142.250.128.95]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00653-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00653-01.pdf	



CSIRT advierte campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00654-01
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 redirección	
https://razapotenew[.]com/activacion/cuenta-wdsh/	
URL sitio falso	
https://rotafonorpp[.]com/1669040910/imagenes/_personas/home/default.asp	
Dirección IP	
[190.107.176.120]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00654-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00654-01.pdf	



CSIRT alerta de campaña de phishing que suplanta un inicio de correo	
Alerta de seguridad cibernética	8FPH22-00655-01
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 redirección	
https://ipfs.io/ipfs/QmTt7qvB3hQF6bYLvwSMR3bydefBagFykXV58vvM5c5QfE?filename=E%20S%20K%20U%20Y%20P%20AU%20BB.html#test@csirt.gov.cl	
URL sitio falso	
https://ipfs.io/ipfs/QmTt7qvB3hQF6bYLvwSMR3bydefBagFykXV58vvM5c5QfE?filename=E+S+K+U+Y+P+AU+BB.html&err=LURN5OTZOPUZ2XNTWIW&dispatch=088&id=8B050622B09b1b8B571291A540a881#test@csirt.gov.cl	
Dirección IP	
[209.94.90.1]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00655-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00655-01-1.pdf	

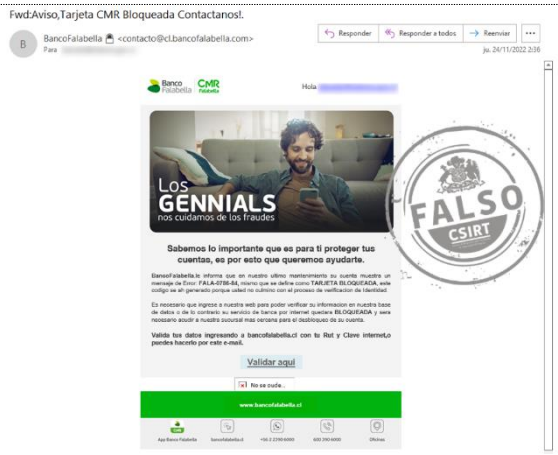


CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00656-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3tQufO9?l=www.bancoripley.cl http://liferfuneral[.]com/wp-includes/certificates/enviar02.php?l=1230969327 https://liferfuneral[.]com/wp-includes/certificates/enviar02.php https://web.bancoripley[.]cl.viverbem.org.br/	
URL sitio falso	
https://web.bancoripley.cl.viverbem[.]org.br/1669120758/login	
Dirección IP	
[5.254.41.129]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00656-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00656-01.pdf	

CSIRT alerta por nueva campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00657-01
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 redirección	
http://cnct[.]us/64AR7h	
URL sitio falso	
https://ingreso-portalcllente-bdchile.cl.murillovp.com[.]br/1669229388/bcochile-web/persona/login/index.html/login	
Dirección IP	
[162.241.203.61]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00657-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00657-01.pdf	

CSIRT alerta de campaña de phishing con falso inicio de sesión de correo	
Alerta de seguridad cibernética	8FPH22-00658-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2022
Última revisión	24 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://j89748889-myjino-ru.translate.goog/?_x_tr_sch=http&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp#test@csirt.gov.cl	
URL sitio falso	
https://m5hxcvt6tps3a6ubllbd4j3duscymke5kjvko2rkuy-ipfs-nftstorage-link.translate.goog/?_x_tr_hp=bafkreif7s4tscxct&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp#test@csirt.gov.cl	
Dirección IP	
[108.177.121.132]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00658-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00658-01.pdf	

CSIRT alerta ante campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00659-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2022
Última revisión	24 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://razapotenew[.]com/activacion/cuenta-wdsh/	
URL sitio falso	
https://persondivou[.]site/1669295861/imagenes/_personas/home/default.asp	
Dirección IP	
[47.87.146.254]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00659-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00659-01.pdf	



CSIRT alerta ante campaña de phishing que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FPH22-00660-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2022
Última revisión	24 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://wedsys.com[.]br/falabella/cuenta-jpvz/ https://bancofalabella.cl.boxofficekhoraki[.]com/login	
URL sitio falso	
https://persondivou[.]site/1669295861/imagenes/_personas/home/default.asp	
Dirección IP	
[185.83.208.139]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00660-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00660-01.pdf	

3. Ataques de Fuerza Bruta

CSIRT alerta de ataques de fuerza bruta contra SMTP	
Alerta de seguridad cibernética	4IIA22-00055-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2022
Última revisión	21 de noviembre de 2022
Indicadores de compromiso	
Direcciones IP	
103.14.224.25	
103.14.225.215	
37.139.128.9	
186.179.100.0	
103.85.204.98	
45.179.169.107	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iia22-00055-01/	
https://www.csirt.gob.cl/media/2022/11/4IIV22-00055-01.pdf	

4. Vulnerabilidades

CSIRT informa de parches para vulnerabilidades en Atlassian BitBucket y Crowd	
Alerta de seguridad cibernética	9VSA22-00747-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2022
Última revisión	22 de noviembre de 2022
CVE	
CVE-2022-43781 CVE-2022-43782	
Fabricantes	
Atlassian	
Productos afectados	
Bitbucket Server and Data Center 7 y 8. Crowd 3.0.0. y posteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00747-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00747-01.pdf	

CSIRT informa de parches para vulnerabilidades en algunos productos Fortinet	
Alerta de seguridad cibernética	9VSA22-00748-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2022
Última revisión	24 de noviembre de 2022
CVE	
CVE-2022-40684	
Fabricantes	
Fortinet	
Productos afectados	
FortiOS: 7.0.0 a 7.2.1. FortiProxy: 7.0.0 a 7.2.0. FortiSwitchManager: 7.2.0, 7.0.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00748-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00748-01.pdf	

5. Concientización

Ciberconsejos para protegerse de la violencia de género en línea

A lo largo de la historia, las mujeres siempre han sido víctimas de violencia, y peor aún, hoy en día las agresiones no se viven solamente en situaciones de la vida física, sino que también está presente en el mundo virtual. Como cada año, este 25 de noviembre se conmemoró el "Día Internacional de la Eliminación de la Violencia contra la Mujer", por esto compartimos los siguientes ciberconsejos para apoyar a la prevención.

Pueden encontrar la campaña completa aquí, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-violencia-de-genero-2/

6. 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.

7. 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.

- José Ignacio Ávila Silva
- Christian Abarca
- Eduardo Toro