Ministerio del Interior y Seguridad Pública

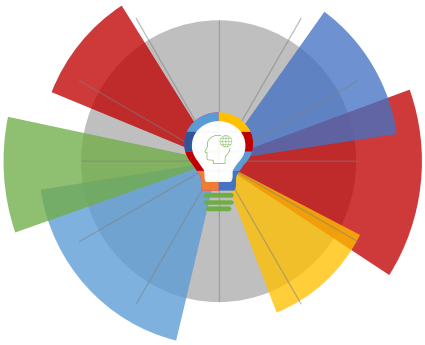
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

25-02-2022 | Año 4 | N°138

Boletín de Seguridad Cibernética

Semana del 18 al 24 de febrero de 2021

La semana en cifras



Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

1

para vulnerabilidades

Las mitigaciones son útiles en productos de Adobe.

IP

4

Informadas

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

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

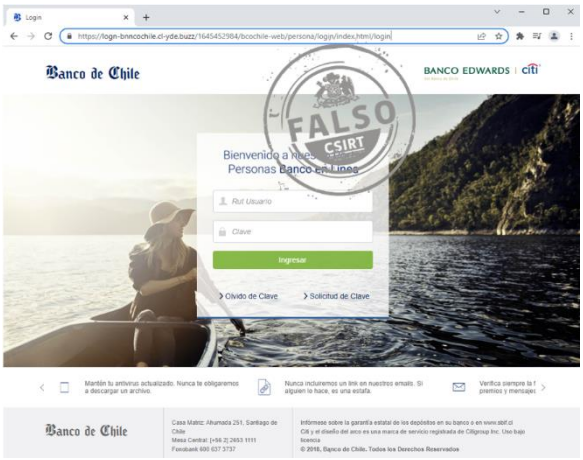
Phishing

CSIRT alerta campaña de phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00476-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2022
Última revisión	22 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://itauapp.canjea-empresas-y-personas[.]com/726a292db52f7f5/html/index.php	
IP	
[104.21.11.32]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00476-01/	
https://www.csirt.gob.cl/media/2022/02/8FPH22-00476-01.pdf	

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

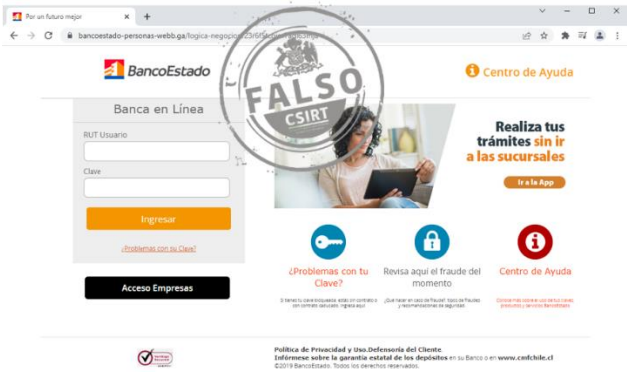
Sitios fraudulentos

CSIRT alerta de nueva página fraudulenta que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01054-01
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 2022
Última revisión	21 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://wwwbancoestado-cl.judithmartens[.]nl/	
IP	
[185.69.233.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01054-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01054-01.pdf	

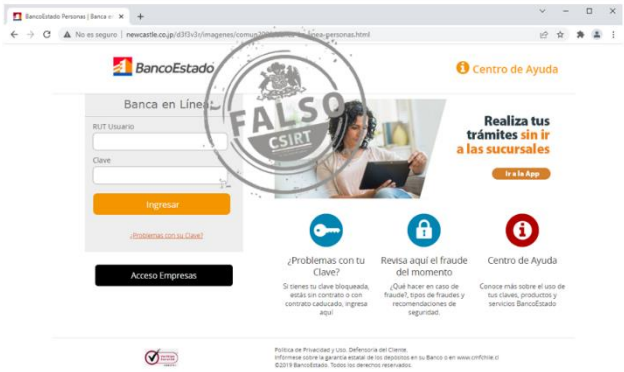


CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01055-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2022
Última revisión	8 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://logn-bnncochile.cl-yde[.]buzz/	
IP	
[172.67.205.202]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01055-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01055-01.pdf	

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob



CSIRT alerta ante nueva página fraudulenta que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01056-01
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 2022
Última revisión	21 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
https://bancoestado-personas-webb[.]ga/logica-negocios?23r6f5tcgim7aql63mja	
IP	
[111.90.143.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01056-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01056-01.pdf	



CSIRT alerta sobre nuevo sitio web fraudulento que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR22-01057-01
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 2022
Última revisión	21 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	
http://newcastle.co[.]jp/d3f3v3r/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[1.33.169.198]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01057-01/	
https://www.csirt.gob.cl/media/2022/02/8FFR22-01057-01.pdf	

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Vulnerabilidades

CSIRT alerta de una nueva vulnerabilidad crítica en Adobe Commerce y Magento	
Alerta de seguridad cibernética	9VSA22-00580-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2022
Última revisión	21 de febrero de 2022
CVE	
CVE-2022-24087	
Fabricante	
Adobe	
Productos afectados	
Adobe Commerce 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores. Magento Open Source 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00580-01/	
https://www.csirt.gob.cl/media/2022/02/9VSA22-00580-01-1.pdf	

Actualidad

Ciberconsejos para lograr comunidades educativas más seguras

Vuelven las clases y con ello la importancia de mantener seguras nuestras comunidades educativa, una responsabilidad de todos, alumnos, apoderados y las escuelas. Por eso les dejamos con recomendaciones clave en los Ciberconsejos de esta semana. Los pueden descargar y compartir en PDF: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-comunidades-educativas/.

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (csirt.gob.cl o al 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Bárbara Palacios
- Kevin Anguita
- Christian Campodónico
- Carlos Humberto de la Fuente Castro