CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 213

semana del 28 de julio al 3 de agosto de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

11

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

20

Las mitigaciones son útiles en productos de Mozilla, Atlassian, Ubuntu y Zimbra.

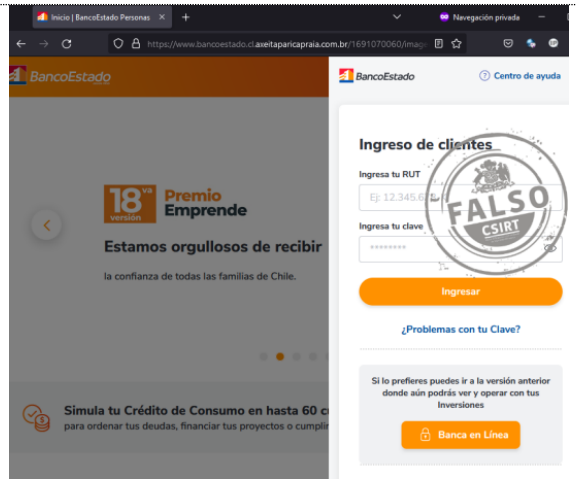
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

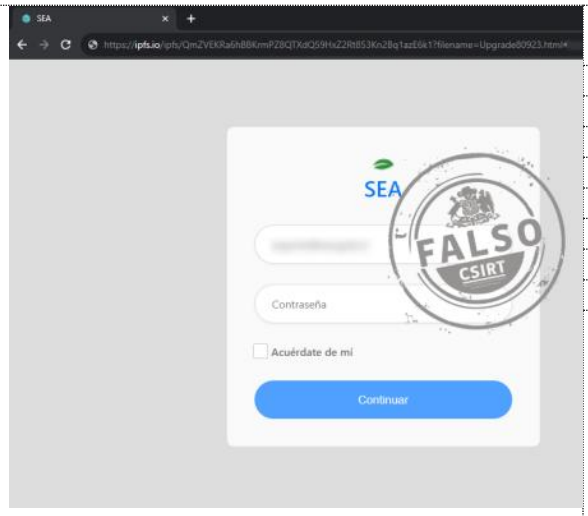
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01479-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://is[.]gd/CYkDn3	
URL sitio falso	
https://cl.correosaddress[.]top/	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01479-01/	

CSIRT alerta de sitio fraudulento que suplanta al Supermercado Rofil	
Alerta de seguridad cibernética	8FFR23-01480-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://supermercado-rofil.webnode[.]page/ https://supermercado-rofil6.webnode[.]page/	
Dirección IP	
[217.16.182.250] [85.132.152.223]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01480-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01481-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.bancoestado.cl.axeitaparicapraia[.]com.br/1691070060/imagenes/_personas/home/default.asp	
Dirección IP	
[192.185.131.48]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01481-01/	

2. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta un inicio de sesión de correo electrónico	
Alerta de seguridad cibernética	8FPH23-00864-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023
URL redirección	
https://ipfs.io/ipfs/QmZVEKRa6hBBKrmPZ8QTXdQ59HxZ2Rt853Kn2Bq1azE6k1?filename=Upgrade80923.html#test@csirt.gob.cl&c=E,1,EK11F056kt_lPddersxFiIDwKxMHbt4os81NGAldJjrc5hfbRRFXAFzEjzLL3StRBgkdvhF4VoNwDs8PhzfR2ZBQo1eaj5TAb3pb3ykjHEM,&typo=1&data=05|01|test@csirt.gob.cl|77121cea35cf4f45d98808db8f58edd2|b71dc67ef57148469db81264f14ea88b|1|0|638261384379089655|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|0|||&sdata=FK3QQdHosLaKTfqJE7eXB58a1OCrkFnCiKkhnUhDMvQ=&reserved=0	
URL sitio falso	
https://ipfs.io/ipfs/QmZVEKRa6hBBKrmPZ8QTXdQ59HxZ2Rt853Kn2Bq1azE6k1?filename=Upgrade80923.html#test@csirt.gob.cl	
Dirección IP	
[162.240.110.92]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00864-01/	

CSIRT alerta de nueva campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00865-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://correoscl1[.]icu/?token=Gnmn0Kuf5PVfJezf	
URL sitio falso	
https://cutt[.]ly/fwsn4r2G	
Dirección IP sitio falso	
[43.135.156.208]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00865-01/	

CSIRT alerta de nueva campaña de phishing, que amenaza falsamente con revelar datos personales del usuario	
Alerta de seguridad cibernética	8FPH23-00866-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00866-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00867-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3OE47RK?l=www.santander.cl https://www.nationaltreasures.co[.]nz/bancosantander/cuenta-daiu/	
URL sitio falso	
https://banco.santander-cl.infenso[.]hr/1691069564/portada/personas/home.asp	
Dirección IP sitio falso	
[185.58.73.179]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00867-01/	

3. Vulnerabilidades

CSIRT comparte información de vulnerabilidad día cero parchada en Zimbra Collaboration Suite (ZCS)	
Alerta de seguridad cibernética	9VSA23-00873-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023
CVE	
CVE-2023-38750	
Fabricante	
Oracle	
Productos afectados	
Zimbra Collaboration Suite (ZCS) anteriores a ZCS 10.0.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00873-01/	

CSIRT comparte nuevas vulnerabilidades parchadas por Atlassian	
Alerta de seguridad cibernética	9VSA23-00874-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023
CVE	
CVE-2023-22505 CVE-2023-22506 CVE-2023-22508	
Fabricante	
Atlassian	
Productos afectados	
Confluence Data Center and Server Bamboo	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00874-01/	

CSIRT comparte información de dos vulnerabilidades parchadas por Ubuntu	
Alerta de seguridad cibernética	9VSA23-00875-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023
CVE	
CVE-2023-2640 CVE-2023-32629	
Fabricante	
Ubuntu	
Productos afectados	
Ubuntu	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00875-01/	

CSIRT comparte vulnerabilidades parchadas en Google Chrome 115		
Alerta de seguridad cibernética	9VSA23-00876-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	2 agosto, 2023	
Última revisión	2 agosto, 2023	
CVE		
CVE-2023-4045 CVE-2023-4046 CVE-2023-4047 CVE-2023-4048 CVE-2023-4049	CVE-2023-4050 CVE-2023-4051 CVE-2023-4052 CVE-2023-4053 CVE-2023-4054	CVE-2023-4055 CVE-2023-4056 CVE-2023-4057 CVE-2023-4058
Fabricante		
Mozilla		
Productos afectados		
Firefox, Firefox ESR.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00876-01/		

4. Concientización

CSIRT participa de Seminario de Ciberseguridad del Ministerio de Salud

La mañana de este martes, el CSIRT de Gobierno participó del Seminario de Ciberseguridad en Salud, organizado por el Ministerio de Salud y que tuvo lugar en el Auditorio del Edificio Moneda Bicentenario, Teatinos 92.

La presentación del CSIRT fue realizada por su actual jefe, Cristián Bravo Lillo, quien explicó los principales elementos de la propuesta de nueva Política Nacional de Ciberseguridad, y del proyecto de Ley Marco de Ciberseguridad, concentrándose en la institucionalidad de ciberseguridad que espera pueda ser implementada al aprobarse ambos textos. Más información de la jornada: csirt.gob.cl/noticias/csirt-seminario-minsal/.

Ciberconsejos | Precauciones ante el uso de dominios .zip

Recientemente empezaron a ser registrados muchos dominios web que terminan en .zip, los que pueden ser usados por ciberdelincuentes para hacer parecer a sus víctimas que un enlaces malicioso es en realidad un archivo comprimido, facilitando la infección de sus equipos con malware.

Por eso es que en estos nuevos Ciberconsejos hacemos un llamado a ser extra cuidadosos al recibir un correo electrónico o mensaje de cualquier aplicación con lo que parece un descargable .zip, siguiendo estas recomendaciones. Pueden encontrarlo también aquí (incluyendo su versión en PDF): csirt.gob.cl/recomendaciones/ciberconsejos-precauciones-dominios-zip/

Ciberconsejos para una navegación segura con tus hijos

Esta semana publicamos ciberconsejos extra con motivo del Día del Niño. Se los puede revisar completos (son 6 láminas e incluyendo una versión en PDF) en nuestro sitio web dedicado a la campaña: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura-con-tus-hijos-2/.

Ciberdiccionario Volumen 42

Una nueva edición del ciberdiccionario del CSIRT, en esta ocasión con las definiciones para domótica, M2M, ciberresiliencia y machine learning. También los pueden encontrar acá, incluyendo una versión en PDF: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-42/.

5. 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.

6. 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.

- Francisco Contreras
- Héctor Jesús Concha Vera
- César Labbé
- Sugy Nam
- Jair Palma
- Natalia Ninoska Riva Barraza
- Pablo Ignacio Pizarro Cortínez

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.04 16:14:31 -04'00'