



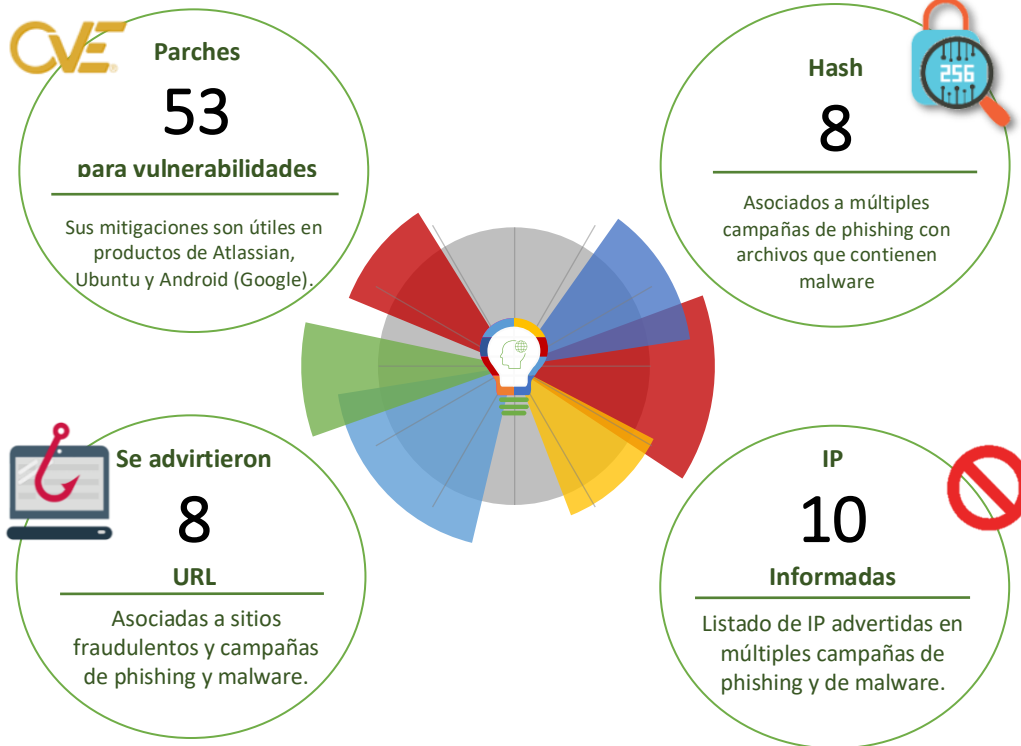
10-06-2022 | Año 4 | N°153

Boletín de Seguridad Cibernética

Semana del 3 al 9 de
junio de 2022



La semana en cifras



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

Contenido

Malware.....	2
Sitios fraudulentos	3
Phishing	4
IoC Ataques de Fuerza Bruta.....	6
Vulnerabilidades	7
Actualidad.....	9
Muro de la Fama	13

Imagen del mensaje

Estimado(A) [redacted].cl

Tesorería General de la República (TGR) informa que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga. Una liquidación tributaria corresponde a la determinación de diferencias de impuesto detectadas por el SII.

Le invitamos a regularizar esta situación a través de nuestro sitio web, en el menú **Recaudación / Pagos / Impuestos Fiscales**, a la brevedad posible, a fin evitar las molestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidas de apremio.

Puede descargar el informe generador por el TGR en el **Adjunto de información**.

Adjuntos de información

Atención: Informe contraseña para ver su PDF. Nunca le des tu contraseña a nadie.
contraseña : 020105

09/06/2022 02:31:37

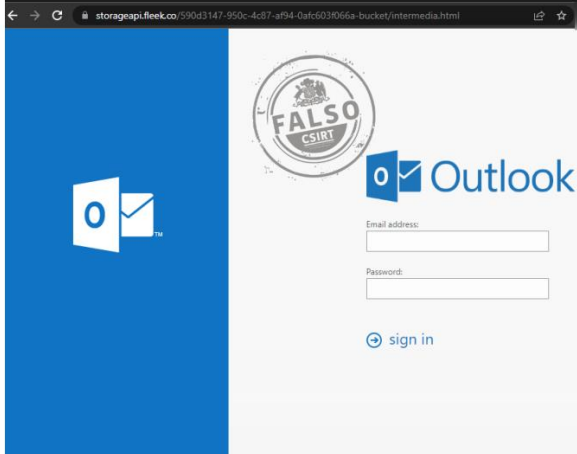


CSIRT advierte phishing con malware suplantando a la TGR

Alerta de seguridad cibernética	2CMV21-00301-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2022
Última revisión	9 de junio de 2022
Indicadores de compromiso	
SHA256	
6a88340516602be1aa9e153ad2394cf1935213fd719cc0e4a378a75f17f051f3dc58e5c807762d9442e4d4b71921c56289081ddc2a367eabad30cca817686fa7cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4e9214d7c92555195443f2ac907302118992f3ea615ee0e0241152327534466c3b988eebe4b1247db6c54519f59ff4e472f0de4b9e85bc6d62c54bfd7a6de394228f24a369fd4c060cb4a77919861c62176a76f87e798b21cde9dc1c93b2af166	
IoC URL	
kiamarketingbuzz.co[.]za inservicedia[.]com anestis[.]info https://kiamarketingbuzz.co[.]za/wp-content/languages/- /https://www.tgr.cl/?cliente=intlohiggins@interior.gob.cl https://inservicedia[.]com/wp-content/uploads/- /TGR00214500011.zip https://anestis[.]info/OLD/images/cloud/V7DX72X8SZDU1QW33.shi	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0301-01/ https://www.csirt.gob.cl/media/2022/06/2CMV22-00301-01.pdf	

Sitios fraudulentos

Imagen del sitio



CSIRT informa sitio web falso de Outlook web	
Alerta de seguridad cibernética	8FFR22-01086-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2022
Última revisión	3 de junio de 2022
Indicadores de compromiso	
URL sitio falso	https://storageapi.fleek[.]co/590d3147-950c-4c87-af94-0afc603f066a-bucket/intermedia.html
IP	[104.18.7.145]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01086-01/
	https://www.csirt.gob.cl/media/2022/06/8FFR22-01086-01.pdf

Phishing

Imagen del sitio



CSIRT advierte phishing con falso concurso que suplanta a COPEC

Alerta de seguridad cibernética	8FPH22-00536-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2022
Última revisión	3 de junio de 2022
Indicadores de compromiso	
URL sitio falso	https://inquirypatch[.]top/VzhMaWQc/copeccl
URL redirección	http://barelysynthesize[.]top/copeccl/tb.php
IP	[104.21.13.232]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00536-01/
	https://www.csirt.gob.cl/media/2022/06/8FPH22-00536-01.pdf

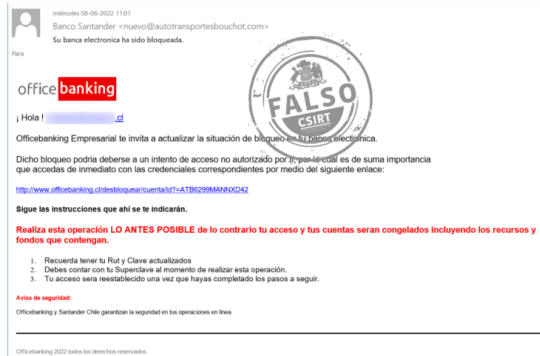
Imagen del sitio



CSIRT alerta de phishing con falso concurso que suplanta a CGE

Alerta de seguridad cibernética	8FPH22-00537-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2022
Última revisión	3 de junio de 2022
Indicadores de compromiso	
URL sitio falso	https://inquirypatch[.]top/snBXDygg/cge-cl
URL redirección	http://anotherbeetle[.]top/cge-cl/tb.php
IP	[172.67.133.106]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00537-01/
	https://www.csirt.gob.cl/media/2022/06/8FPH22-00537-01.pdf

Imagen del mensaje



CSIRT advierte phishing que suplanta a Office Banking del Banco Santander

Alerta de seguridad cibernética	8FPH22-00538-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2022
Última revisión	9 de junio de 2022
Indicadores de compromiso	
URL sitio falso	https://www.offlcebanking.cl.nuniavillabali[.]com/
URL redirección	https://bit[.]ly/3xqPN6L https://yummiss[.]xyz/wp/index.php
IP	[103.253.212.219]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00538-01/
	https://www.csirt.gob.cl/media/2022/06/8FPH22-00538-01.pdf

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Nombre sistema autónomo	Documento web
5.34.207.118	AS 15828	Blue Diamond Network Co., Ltd.	4IIA21-00051-01
5.34.207.123	AS 15828	Blue Diamond Network Co., Ltd.	4IIA21-00051-01
5.34.207.194	AS 15828	Blue Diamond Network Co., Ltd.	4IIA21-00051-01
5.34.207.98	AS 15828	Blue Diamond Network Co., Ltd.	4IIA21-00051-01
103.147.185.238	AS 135905	Vietnam Posts and Telecommunications	4IIA21-00051-01

Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA22-00651-01
CSIRT alerta ante vulnerabilidad crítica en Atlassian Confluence

PARA REGISTRAR | 562 2486 3850
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta ante vulnerabilidad crítica en Atlassian Confluence	
Alerta de seguridad cibernética	9VSA22-00651-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2022
Última revisión	7 de junio de 2022
CVE	
CVE-2022-26134	
Fabricante	
Atlassian	
Productos afectados	
Confluence Server y Data Center, todas las versiones con soporte.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00651-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00651-01.pdf	



INFORME DE Vulnerabilidad

9VSA22-00652-01
CSIRT alerta ante vulnerabilidades crítica en Vim para Ubuntu

PARA REGISTRAR | 562 2486 3850
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta vulnerabilidades en Vim para Ubuntu	
Alerta de seguridad cibernética	9VSA22-00652-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2022
Última revisión	7 de junio de 2022
CVE	
CVE-2022-0554	CVE-2022-0943
CVE-2022-0572	CVE-2022-1616
CVE-2022-0685	CVE-2022-1619
CVE-2022-0714	CVE-2022-1620
CVE-2022-0729	CVE-2022-1621
Fabricante	
Ubuntu	
Productos afectados	
Ubuntu 16.04	
Vin (Ubuntu package) anteriores a 2:7.4.16893ubuntu1.5+esm6	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00652-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00652-01-1.pdf	



INFORME DE Vulnerabilidad

9VSA22-00653-01
CSIRT alerta ante vulnerabilidades de Android para junio de 2022

PARA REGISTRAR | 562 2486 3850
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades de Android para junio 2022		
Alerta de seguridad cibernética	9VSA22-00653-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	7 de junio de 2022	
Última revisión	7 de junio de 2022	
CVE		
CVE-2021-39691	CVE-2022-20137	CVE-2022-20132
CVE-2022-20006	CVE-2022-20142	CVE-2022-20136
CVE-2022-20125	CVE-2022-20144	CVE-2022-21745
CVE-2022-20138	CVE-2022-20147	CVE-2022-20210
CVE-2021-39624	CVE-2022-20123	CVE-2021-35083
CVE-2022-20130	CVE-2022-20131	CVE-2021-35102
CVE-2022-20127	CVE-2022-20129	CVE-2021-35111
CVE-2022-20140	CVE-2022-20143	CVE-2022-22082
CVE-2022-20145	CVE-2021-4154	CVE-2022-22083
CVE-2022-20124	CVE-2022-20141	CVE-2022-22084
CVE-2022-20126	CVE-2022-24958	CVE-2022-22085
CVE-2022-20133	CVE-2022-25258	CVE-2022-22086
CVE-2022-20134	CVE-2022-25258	CVE-2022-22087
CVE-2022-20135	CVE-2022-20132	CVE-2022-22090
Fabricante		
Google		
Productos afectados		
Android, versiones anteriores a la 10		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00653-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00653-01.pdf		

Actualidad

Ciberconsejos para un uso más seguro de TikTok

Para los Ciberconsejos de esta semana entregamos recomendaciones para usar la aplicación TikTok de una forma más segura, reduciendo el riesgo de exponer demasiada información de los niños y adolescentes, que son los principales usuarios de la app, y peligros como el grooming.

Pueden descargar asimismo estas imágenes, compiladas en un único PDF, en nuestro sitio web: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-tiktok/>.



The infographic consists of five cards, each with the CSIRT logo and the title 'CIBERCONSEJOS PARA USAR DE FORMA SEGURA TIKTOK'.
1. **¿Qué es TikTok?**: Describes TikTok as a global social media platform for short videos, popular among users under 30.
2. **Riesgos de TikTok**: Lists risks such as family information exposure, inappropriate content, sexual grooming, cyberbullying, dangerous viral challenges, and data access (contacts, location, microphone, camera).
3. **¿Cómo protegerse?**: Provides steps: 1. Set account to private, 2. Configure profile for private messages/comments, 3. Report abusive accounts, 4. Save evidence of harassment.
4. **¿Qué pueden hacer los padres?**: Provides steps: 1. Ensure age-appropriate social media use, 2. Set consistent limits and talk beforehand, 3. Create secure passwords with children, 4. Talk about risks and teach content discrimination.
5. **¿Qué pueden hacer los padres?**: Provides steps: 5. Activate family synchronization, which allows for: setting viewing time limits, restricting inappropriate content, and managing privacy/security settings.

Ciberdiccionario Volumen 8

En su octava edición, esta semana en el Ciberdiccionario definimos Credenciales, Antispyware, Exfiltración y Defacement. Los encuentran todos también en nuestra web oficial: <https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-8/>.

 <p>Ciber diccionario</p>  <p>Exfiltración: Acción de extraer datos sin autorización desde un sistema electrónico y entregarlos ya sea a personas en específico o libremente a la comunidad. También se llama fuga de información.</p>	 <p>Ciber diccionario</p>  <p>Credenciales: Elementos que emplea el usuario para ingresar a un sistema o sitio web que exige identificación. Usualmente se refiere a usuario y contraseña, comprende otras claves, tokens o combinaciones de autenticación si las hubiera.</p>
 <p>Ciber diccionario</p>  <p>Defacement: Delito en el que se altera sin permiso la web de una persona o empresa, cambiando contenido como mensajes e imágenes. El defacement suele tener fines políticos o de denuncia, haciéndolo también hackers para demostrar su habilidad.</p>	 <p>Ciber diccionario</p>  <p>Antispyware: Programas de software que buscan específicamente identificar y destruir programas maliciosos (malware) de tipo spyware, o sea, aquellos que nos espían y roban nuestra información confidencial.</p>

Ciberconsejos | ¿Qué capacidades debe tener nuestra organización para enfrentar un ciberataque?

Nuestros equipos informáticos o de ciberseguridad deben tener claros sus roles y responsabilidades para enfrentar con rapidez y eficiencia una emergencia o incidente grave que afecte a nuestra empresa o institución. Como referencia, elaboramos un resumen simple con las principales capacidades con las que debemos contar con tal de responder efectivamente ante las amenazas.

Pueden descargarlos en: csirt.gob.cl/recomendaciones/capacidades-ciberataque/.



I. - ACTUAR CON RAPIDEZ

Cada minuto cuenta cuando un malware ha ingresado en nuestros sistemas y está encriptando nuestros datos. Cada miembro de la organización debe tener claro su rol, para no perder tiempo, actuar coordinadamente, y realizar una respuesta eficiente y eficaz al ataque. Hay que actuar rápido, pero en lo posible en base a playbooks escritos y probados, pues un error en la primera respuesta puede costarle muy caro a la institución.

II. - ENTENDER LA SITUACIÓN Y GUIAR A LA ORGANIZACIÓN

Los responsables de ciberseguridad deben comprender el ataque y transmitir información a la organización de modo comprensible y con instrucciones para actuar en la práctica. La primera evaluación debe aportar indicadores preliminares que permitan ponderar la criticidad e impacto del incidente para poner al tanto al jefe de servicio si el incidente pone en riesgo la continuidad operacional de los servicios institucionales o afecta gravemente su reputación.

III. - PROCEDER EFICAZ Y COORDINADAMENTE

Los responsables de ciberseguridad deben manejar, conocer y poder coordinar con los equipos de operaciones la actuación de las diferentes plataformas de control de incidencias dentro de su infraestructura TI, con el objetivo de contener, aislar y mitigar el riesgo lo antes posible. Gracias a que cada uno conoce su rol, el líder de ciberseguridad puede coordinar a los miembros del equipo para que apliquen los planes de la política de ciberseguridad de la organización. En la cadena de coordinación del incidente es clave el cumplimiento normativo de notificación obligatoria al CSIRT de Gobierno y requerir su ayuda si el incidente no se está logrando contener o aislar.

IV. - PROCESAR GRANDES VOLÚMENES DE DATOS

El equipo de ciberseguridad debe ser capaz de procesar un mayor volumen de datos del habitual, para entender los vectores de ataque y puntos calientes del malware, con el objetivo de responder al ciberataque y mantener la disponibilidad de sus servicios. Contemplar necesidad de obtener capacidad en la nube y apoyo de unidades análisis automatizados basados en IA, para aliviar y acelerar el procesamiento masivo de información que provendrá de múltiples dispositivos.

V. - JUDICIALIZAR

Tenga presente que un incidente puede llegar a clasificarse posteriormente como un delito informático, razón por la cual dentro del protocolo de respuesta a incidentes deben estar incluidas las consideraciones para no afectar la evidencia o pruebas digitales que servirán posteriormente para judicializar el delito. Pruebas digitales bien preservadas podrán usarse ante un juicio y tendrán el mismo valor probatorio que una evidencia física, y ayudarán a la fiscalía y policías a encontrar a los responsables.

¿Estás preparado?

CSIRT
<https://www.csirt.gob.cl/>
Teatinos 92 piso 6
Santiago, Chile

1510
@CSIRTSGB
<https://www.linkedin.com/company/csirt-gob>
<https://www.instagram.com/compacib>

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.



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 (<https://www.csirt.gob.cl> o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Carlos Escalona Peraza
- Natalia Medina
- David Soto
- Mathias Roco Fernández
- María Gabriela Fernández
- Gonzalo Andrés Araya Navarrete
- Gisela Araya
- Nicolás Ramírez
- Erick Reyes Torres

