Ministerio del Interior y Seguridad Pública

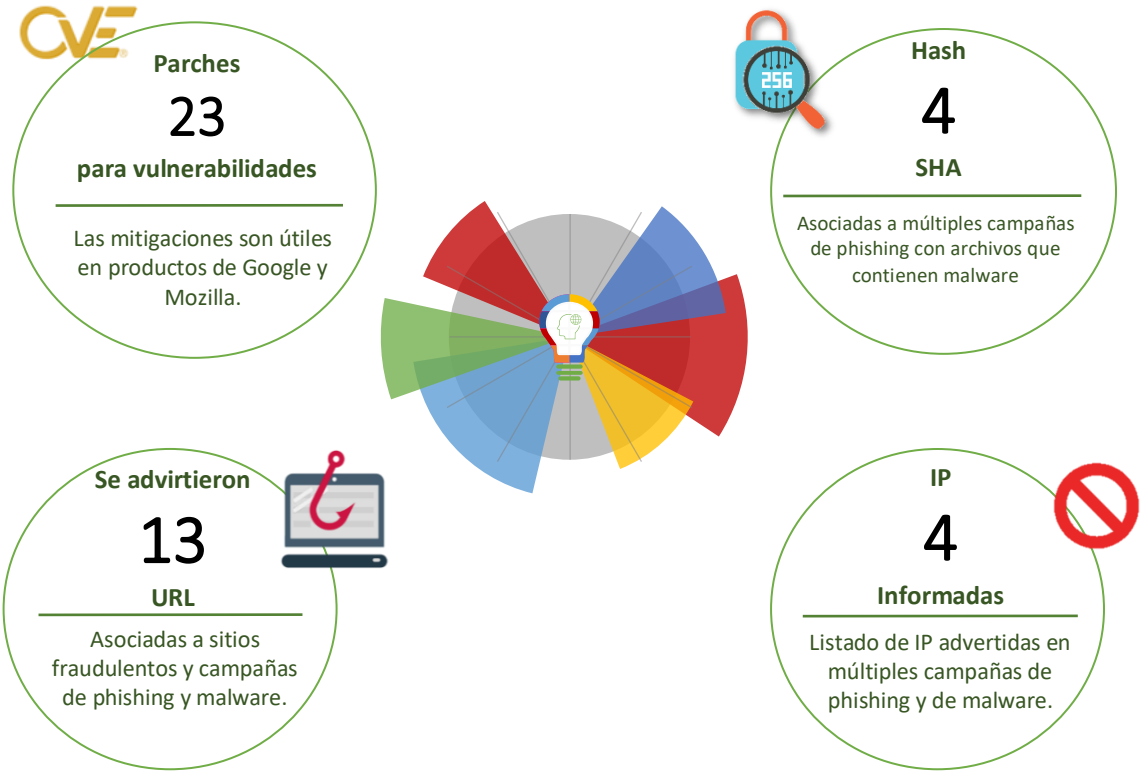
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

08-07-2022 | Año 4 | N°157

Boletín de Seguridad Cibernética

Semana del 1 al 7 de julio 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

Imagen del Mensaje

CSIRT alerta de nueva campaña de phishing con malware Emotet	
Alerta de seguridad cibernética	2CMV21-00305-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Julio de 2021
Última revisión	05 de Julio de 2021

Indicadores de compromiso

SHA256

Nombre: comentarios_05072022.zip
SHA256:
2a719f016808a55a5030a572c555859f57bc72dcc1b42d9a3a0d083e3ec29272

Nombre: comentarios_05072022.xls
SHA256:
3db2ab1966f944f46e4cb802f2d4e71d407d989766c20809d232552fe55d29d1

Nombre: GMzFuprDxRwN4hl.dll
SHA256:
1f61283047a973092a6c15d8bb589c40a414e662ca100abf2bc176289b756715

Nombre: lff61byugTX68nr.dll
SHA256:
9c2846b8e877f8bfdb83bc129ee32ec50bc3515462fb6ae0d303a4528d7115d5

IoC URL

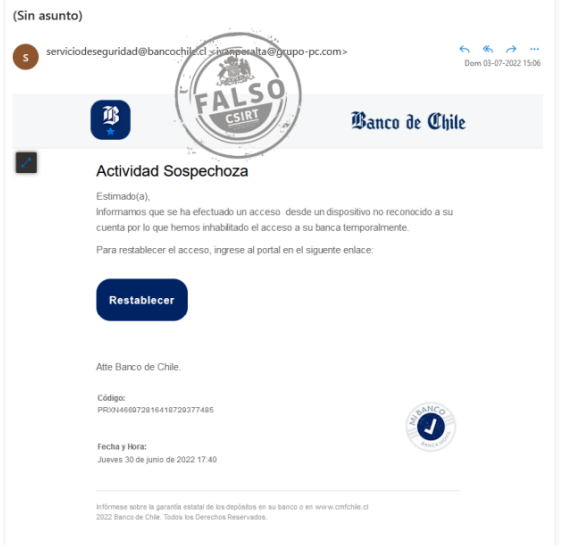
flywithme[.]dk
clinicaportalpsicologia.com[.]br
greenlizard.co[.]za
fundaciontheoz[.]cl
https://flywithme[.]dk/wp-includes/xFbL/
http://www.clinicaportalpsicologia.com[.]br/wp-content/rknwta6Ncgt9xnXu7S/
https://greenlizard.co[.]za/amanah/HJErj/
http://www.fundaciontheoz[.]cl/pensamientooccidental/tilKftYVgHoCu4pp

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-00305-01/
https://www.csirt.gob.cl/media/2022/07/2CMV22-00305-01.pdf

Phishing

Imagen del mensaje



CSIRT informa phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00550-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de julio de 2022
Última revisión	4 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3boeqIu https://gocloudasiaacademe[.]com/?id=28	
URL sitio falso	
https://login.acceso-portal.bancochlle.cl.mutmobila[.]ro/1656942540/bcochileweb/persona/login/index.html/login	
IP	
[45.91.4.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00550-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00550-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00551-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de julio de 2022
Última revisión	6 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3Aoob46?l=www.santander.cl http://brombalplatform[.]com/disegnatori/bootstrap/enviar03.php?l=293441200 https://bit[.]ly/3OOsY30?l=www.santander.cl https://gurujam[.]com/activacion/cuenta-dwis/	
URL sitio falso	
https://banco.santander.cl.smajbazar[.]ir/1657122327/portada/personas/home.asp	
IP	
[88.99.137.77]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00551-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00551-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00552-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de julio de 2022
Última revisión	6 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3NLpbSS hXXp://139.59.7.115/8b333af2b5b820568d666016a0bbc9a0/e98ef2fcdbc0f740d30f01ac1f780d85/05c16bSUrY?31139769	
URL sitio falso	
https://creditos-bancoestado[.]gq/extranjeros?2536c52f56dl56m36im3g7q	
IP	
[204.11.58.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00552-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00552-01.pdf	

CSIRT advierte phishing que suplanta a una oficina de correos	
Alerta de seguridad cibernética	8FPH22-00553-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de julio de 2022
Última revisión	7 de julio de 2022
Indicadores de compromiso	
URL Redirección	
http://sz5[.]me/98laYE https://sweetgift[.]live/ips_cl/?cep=	
URL sitio falso	
https://www.claimprize[.]site/lander_cl_rewards-2/?x_txid=62c72e57e0a4db033f5dd7f8&x_sub_id=1027_2446_2446&x_click_id=62c72e57e0a4db033f5dd7f8	
IP	
[34.205.248.193]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00553-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00553-01.pdf	

Vulnerabilidades

CSIRT comparte información de vulnerabilidades parchadas Firefox 102		
Alerta de seguridad cibernética	9VSA22-00669-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	4 de julio de 2022	
Última revisión	4 de julio de 2022	
CVE		
CVE-2022-34470	CVE-2022-34481	CVE-2022-34480
CVE-2022-34468	CVE-2022-34474	CVE-2022-34477
CVE-2022-34479	CVE-2022-34469	CVE-2022-34475
CVE-2022-34484	CVE-2022-34471	CVE-2022-34473
CVE-2022-34482	CVE-2022-34472	CVE-2022-34484
CVE-2022-34483	CVE-2022-34478	CVE-2022-34485
CVE-2022-34476	CVE-2022-2200	
Fabricantes		
Mozilla Firefox		
Productos afectados		
Mozilla Firefox, versiones anteriores a la 102		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00669-01/		
https://www.csirt.gob.cl/media/2022/07/9VSA22-00669-01-1.pdf		

CSIRT informa actualización Google Chrome 103	
Alerta de seguridad cibernética	9VSA22-00667-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de julio de 2022
Última revisión	5 de julio de 2022
CVE	
CVE-2022-2294	
CVE-2022-2295	
CVE-2022-2296	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones anteriores a la 103.0.5060.114.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00670-01/	
https://www.csirt.gob.cl/media/2022/07/9VSA22-00670-01.pdf	

Actualidad

VIDEO | Ciberconsejos para evitar el robo de WhatsApp

El robo de cuentas de WhatsApp se está convirtiendo en una forma cada día más utilizada por los ciberdelincuentes para suplantar la identidad de la víctima y robar dinero. ¿Qué técnicas utilizan los delincuentes y cómo prevenir?

Lo anterior, lo explicamos nuestro nuevo video publicado esta semana que termina y disponible en https://www.csirt.gob.cl/recomendaciones/secuestro-de-whatsapp/ (desde donde también es posible descargarlo fácilmente) y también el canal de YouTube del CSIRT de Gobierno: https://www.youtube.com/watch?v=8kKyCBrim7Y.

Ciberdiccionario Volumen 10

En esta edición X del Ciberdiccionario, hablamos de dispositivos que se transforman zombies, de huellas digitales que no están en nuestros dedos, de firmas que permiten identificar a programas maliciosos y de los comandos que explotan vulnerabilidades. Pueden ver estas definiciones también en PDF aquí: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-10/

Ciberconsejos | Qué son los incidentes de ciberseguridad y cómo reportarlos

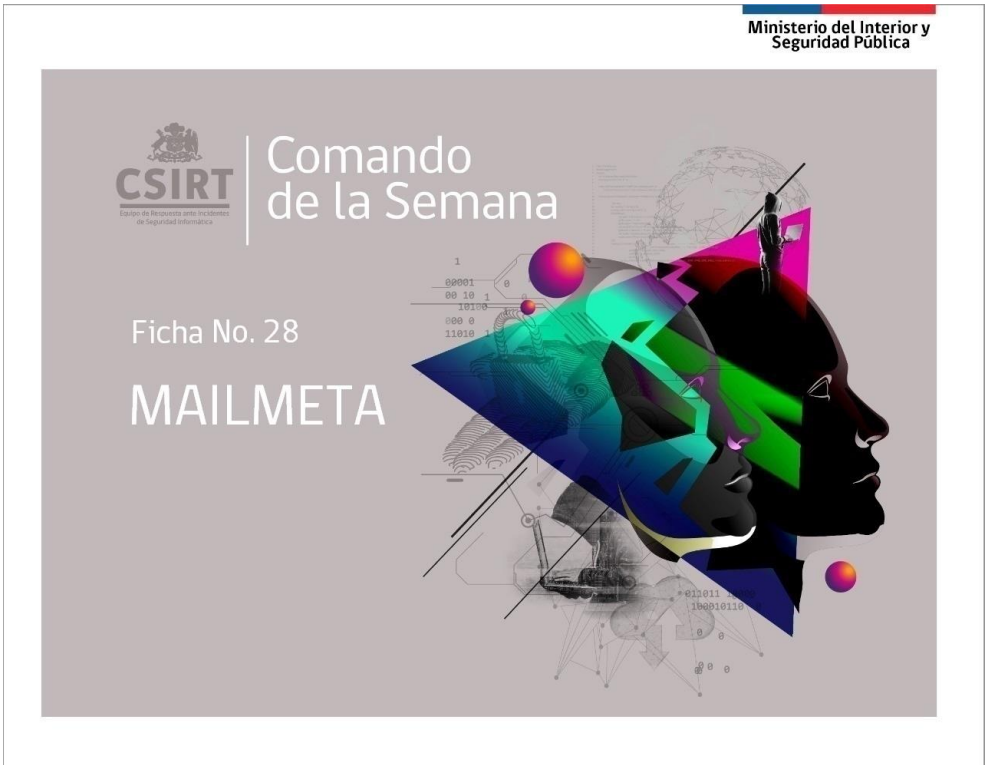
Porque la ciberseguridad es un trabajo de todos, compartimos en esta ocasión una guía sencilla para que puedas identificar varios tipos de incidente de ciberseguridad, con especial detalle en el phishing, y reportarlos a nosotros en el CSIRT de Gobierno, ya sea a través del formulario en csirt.gob.cl o llamando al 1510.

Pueden descargar la guía aquí: https://www.csirt.gob.cl/recomendaciones/incidentes-y-como-reportarlos/.

El Comando de la Semana | No. 28 MailMeta

El Comando de la Semana en esta ocasión les trae a MailMeta, una herramienta forense basada en Python que lee las cabeceras de los archivos de correo electrónico y extrae información crucial para identificar si el email es legítimo.

Descarga el Comando de la Semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-28/.



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 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.

- Guillermo Carrillo
- Bárbara Palacios
- Edwin Durán
- David Soto
- Jean Catalán
- Pablo Christiny Mujica
- Camila Paz Gizzi Ramírez
- Hanz Sandoval
- Javier Karmy Selman
- Óscar Ahumada Godoy
- Raúl Beyzaga