Ministerio del Interior y Seguridad Pública

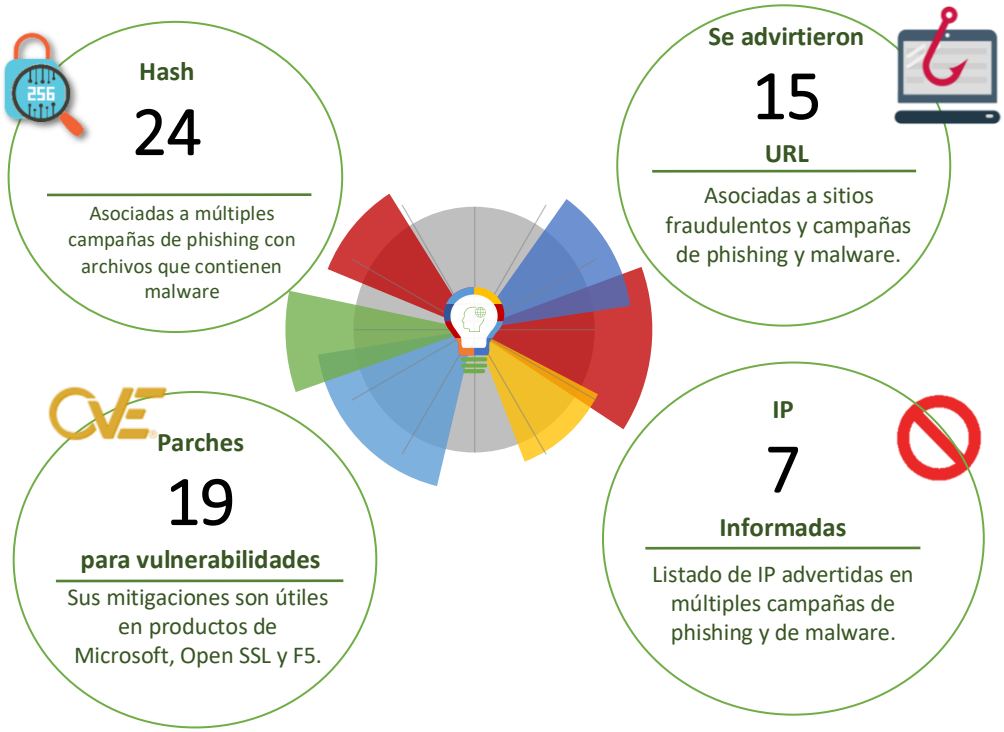
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

06-05-2022 | Año 4 | N°148

Boletín de Seguridad Cibernética

Semana del 29 de abril
al 5 de mayo de 2022

La semana en cifras



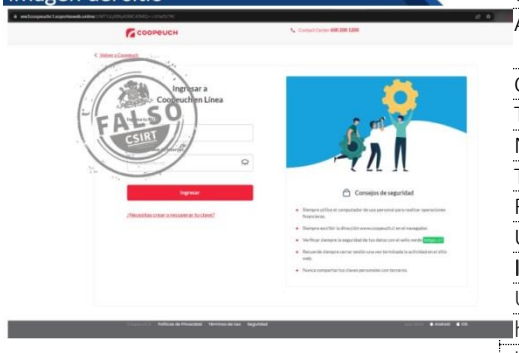
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

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

Sitios fraudulentos

Imagen del sitio



CSIRT informa página web que suplanta al de Coopeuch	
Alerta de seguridad cibernética	8FFR22-01080-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2022
Última revisión	29 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://www.uniformesmussa[.]com/	
hXXps://ww3coopeuchc1.soportesweb[.]online/l/MTYzLjI0Ny43MC43MQ==/l/tef3/?#/	
IP	
[172.105.252.225]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01080-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01080-01.pdf	

Phishing

Imagen del mensaje

CSIRT informa phishing con falsa tarjeta bloqueada	
Alerta de seguridad cibernética	8FPH22-00517-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
Indicadores de compromiso	
URL redirección	
https://serviciservis[.]com/Centro_ayuda/cuenta-wabz/	
URL sitio falso	
https://sixthstartech[.]com/cmfchil/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[101.53.141.67]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00517-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00517-01.pdf	

Imagen del mensaje

CSIRT alerta phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00518-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/	
URL sitio falso	
hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[190.114.253.236]	
[138.128.170.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00518-01-2/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00518-01.pdf	

Imagen del mensaje

CSIRT advierte phishing con falsa cuenta suspendida	
Alerta de seguridad cibernética	8FPH22-00519-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
Indicadores de compromiso	
URL redirección	
https://kaukaparaiso[.]com/ganador/cuenta-ozli/	
URL sitio falso	
https://nsp.kendranew[.]com/1651501451/Login	
IP	
[168.232.165.180]	
[138.128.170.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00519-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00519-01.pdf	

Imagen del mensaje

CSIRT advierte phishing a través de Facebook Messenger	
Alerta de seguridad cibernética	8FPH22-00520-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://youtube.ve4y[.]com/qgl2fu1	
URL sitio falso	
hXXps://ranzer-gost.format[.]com/	
IP	
[104.18.134.62]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00520-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00520-01.pdf	

Malware


Imagen del mensaje

Estimado(A)

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

Le invitamos a regularizar esta situacion a traves de nuestro sitio web, en el menu **Recaudacion / 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 Adjuntos de información.

Adjuntos de información

FALSO

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

02/05/2022 12:51:40

CSIRT advierte campaña con malware que suplanta a la TGR	
Alerta de seguridad cibernética	2CMV21-00296-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
Indicadores de compromiso	
SHA256	
03840e262fc8208312074c8c0cc5790c586516c1d36536425f52a0768d69021e 9181e3ecde1ea8f60d4eb0c16f760c51a3f099766bcca1eb9ad19136894a5ada bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f 16addd40397c045ed4c393f83443a10cb583171e2fe1f95782e06276db474adb 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 880a365b8d47729b16359bd90136ecbc176e3191eba9a7f18f6285a0cf624620 ea972fdc38c685ace5c5a23b849ac673825e7e4d257bb5b06312ec43c1645400 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 610ce9c0087f8b7a87cb839efe47338121d5681d4a4bd8f248acfc6c29969c47	
IoC URL	
https://physionormandie[.]com/wp-content/languages/–/https:/www.tgr.cl https://www.tri-techmechanical[.]com/components/com_config/dad/HD812U1NDS71Y[.]zip	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00296-01/	
https://www.csirt.gob.cl/media/2022/05/2CMV22-00296.pdf	

CSIRT advierte phishing con malware suplantando a TGR	
Alerta de seguridad cibernética	2CMV21-00297-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022

Indicadores de compromiso

SHA256

4a2d4e8907797a94e5cd032cc67c7a1116f9f640c6aaed531afc60578385adf5
20eb84bc76f6da4eff41a66dfcc0b4c5372233d1568f73d701b9f9f8e8c98da1
2182ac079032bc9e21f20646ff5be6f9a8536a70ce2824b1c2783178e8f2f723
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967
bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
8941f7cc75ae085f5b45c94b831ecc0f8a2aeba792d75b98292660feda2b8775
fd99e83a1161f3cf6bc07f5f973d0272e42e7f1aa9fa7ae22c9c9b1378b3d6c5
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
5ee419a1bda6b3d9ed3c5ffcaa2b4763bd7e7c57d40caa4f89ceebcd689ac840

IoC URL

hXXps://physionormandie[.]com/wp-content/languages/–/https:/www.tgr.cl/?cliente=
hXXps://www.stt.eesc.usp[.]br/wp-content/languages/SII63301220.zip
hXXps://www.hardam[.]biz/stats/awsindex/TD821YEJSDM813UJR.zip

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-00297-01/
https://www.csirt.gob.cl/media/2022/05/2CMV22-00297.pdf

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en Microsoft Edge	
Alerta de seguridad cibernética	9VSA22-00627-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de mayo de 2022
Última revisión	3 de mayo de 2022
CVE	
CVE-2022-1314 - CVE-2022-1313 - CVE-2022-1312 CVE-2022-1310 - CVE-2022-1308 - CVE-2022-1307 CVE-2022-1306 - CVE-2022-1305 - CVE-2022-1364 CVE-2022-1309	
Fabricante	
Microsoft	
Productos afectados	
Microsoft Edge (Chromium-based): 79.0.309.71 – 100.0.1185.39.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00627-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00627-01.pdf	

CSIRT alerta de vulnerabilidades en OpenSSL	
Alerta de seguridad cibernética	9VSA22-00628-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022
CVE	
CVE-2022-1292 - CVE-2022-1343 - CVE-2022-1434 CVE-2022-1473 Impacto CVE-2022-1292: Moderado CVE-2022-1343: Moderado CVE-2022-1434: Bajo CVE-2022-1473: Bajo	
Fabricante	
OpenSSL	
Productos afectados	
OpenSSL versiones 1.0.2, 1.1.1 y 3.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00628-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00628-01.pdf	

CSIRT alerta de vulnerabilidad crítica en BIG-IP de F5	
Alerta de seguridad cibernética	9VSA22-00629-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de mayo de 2022
Última revisión	5 de mayo de 2022
CVE	
CVE-2022-1388	
Fabricante	
F5	
Productos afectados	
BIG-IP, versiones: 16.1.0 a 16.1.2 15.1.0 a 15.1.5 14.1.0 a 14.1.4 13.1.0 a 13.1.4 12.1.0 a 12.1.6 (no serán parchados) 11.6.1 a 11.6.5 (no serán parchados)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00622-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00622-01.pdf	

Actualidad

Ciberconsejos | Browser In The Browser (BITB), la nueva técnica que dificulta identificar un phishing

Una de las técnicas más utilizadas por los ciberdelincuentes es el phishing, la que busca engañar a sus víctimas con correos o páginas web falsas, con el objetivo de inyectar programas maliciosos u obtener los datos personales de los usuarios, como claves bancarias o de redes sociales y así robarles dinero o suplantarlos en internet, entre otros delitos.

Y así como los sistemas de ciberseguridad han ido mejorando, las técnicas de phishing también han evolucionado. Un ejemplo de esto es la técnica conocida como Browser in the Browser (BITB).

Enlace: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-bitb/

Ciberconsejos | Decálogo de Ciberseguridad

Como CSIRT de Gobierno, sabemos bien que la ciberseguridad depende de todos. Por eso, es esencial que tengamos siempre presentes algunas reglas básicas para estar más seguros en línea.

Es con ese objetivo que diseñamos el siguiente Decálogo de Ciberseguridad, diez consejos que todos debemos conocer, indispensables para tener una vida digital más segura.

Enlace: https://www.csirt.gob.cl/recomendaciones/decalogo-de-ciberseguridad/.

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.

- Nicolás Moreno
- César López
- David Soto
- Juan Alfonso Muñoz