Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

02-07-2021 | Año 3 | N°104

Boletín de Seguridad Cibernética

Semana del 25 de junio al 1 de julio de 2021

La semana en cifras

Hash

23

SHA

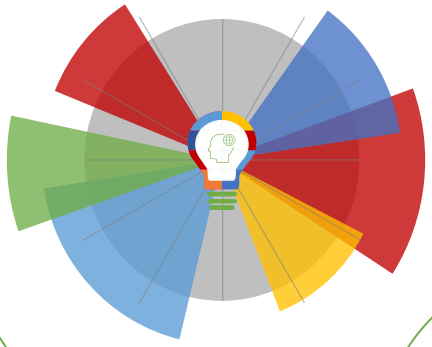
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

7

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

4

para vulnerabilidades

Las mitigaciones son útiles en productos de Trend Micro y Western Digital.

IP

19

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

Malware

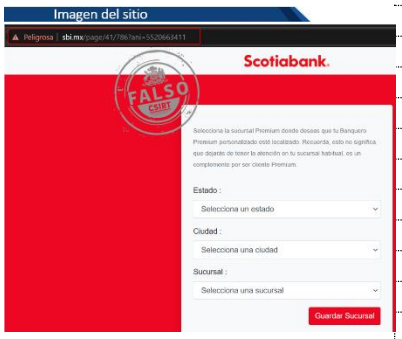
CSIRT alerta ante campaña de malware con phishing que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00199-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2021
Última revisión	29 de junio de 2021
Indicadores de compromiso	
SHA256	
B7F246E869215B5FF134341CD1AB085594C0B532B173D902ACEBE1F3DC213236 77E19EEB9AC37EFB541EF647F401A372F5ED2098690156AE6A42AE65B906DEA6	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00199-01/	
https://csirt.gob.cl/media/2021/06/2CMV21-00199-01.pdf	

Sitios fraudulentos

Imagen del sitio

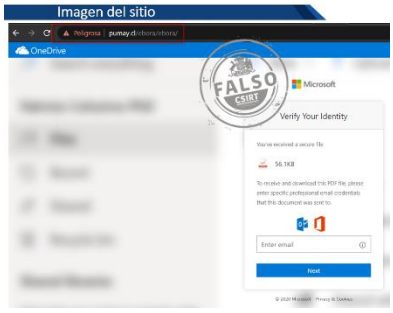
CSIRT alerta ante sitio fraudulento que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR21-00983-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de junio de 2021
Última revisión	30 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
hXXp://221.150.115.216/wordpress/wp-content/php/931af583573227f0220bc568c65ce104/	
IP	
[221.150.115.216]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00983-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00983-01.pdf	

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta a Scotiabank	
Alerta de seguridad cibernética	8FFR21-00984-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de junio de 2021
Última revisión	30 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://sbi[.]mx/page/41/786?ani=5520663411	
IP	
[64.251.8.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00984-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00984-01.pdf	

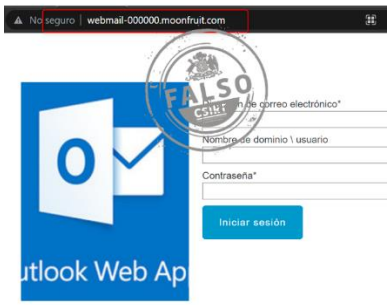
CSIRT alerta ante página fraudulenta que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR21-00985-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de junio de 2021
Última revisión	30 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://cbl57.csb[.]app/index.html	
IP	
[104.18.26.114]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00985-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00985-01.pdf	



CSIRT alerta ante página fraudulenta que suplanta a OneDrive	
Alerta de seguridad cibernética	8FFR21-00986-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de julio de 2021
Última revisión	1 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
https://pumay[.]cl/ebora/ebora/	
IP	
[200.29.0.33]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00986-01/	
https://www.csirt.gob.cl/media/2021/07/8FFR21-00986-01.pdf	

Phishing

Imagen del sitio



CSIRT alerta de campaña de phishing con falsa migración de Outlook	
Alerta de seguridad cibernética	8FPH21-00415-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de julio de 2021
Última revisión	1 de julio de 2021
Indicadores de compromiso	
URL sitio falso	
http://webmail-000000.moonfruit[.]com/	
IP	
[34.255.56.68]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00415-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00415-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00416-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de julio de 2021
Última revisión	1 de julio de 2021
Indicadores de compromiso	
URL de SMS	
https://bit[.]ly/MiPass-cl	
URL sitio falso	
https://porrtalperrsonas-lbancochiile.cl-tyees[.]xyz/1625168391/bcochile-web/persona/login/index.html/login	
IP	
[104.21.91.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00416-01/	
https://www.csirt.gob.cl/media/2021/07/8FPH21-00416-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades críticas en WD My Book y llama a desconectarlos de internet	
Alerta de seguridad cibernética	9VSA21-00460-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de junio de 2021
Última revisión	30 de junio de 2021
CVE	
CVE-2021-35941 CVE-2018-18472	
Fabricante	
Western Digital	
Productos afectados	
WD My Book Live: Todos WD My Book Live Duo: Todos	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00460-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00460.01.pdf	

CSIRT alerta por vulnerabilidades graves en Trend Micro Password Manager	
Alerta de seguridad cibernética	9VSA21-00461-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de julio de 2021
Última revisión	1 de julio de 2021
CVE	
CVE-2021-32461 CVE-2021-32462	
Fabricante	
Trend Micro	
Productos afectados	
Password Manager for Windows: 3.8.0.1103, 5.0.0.1076, 5.0.0.1081, 5.0.0.1217, 5.0.1058	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00486-01	
https://www.csirt.gob.cl/media/2021/07/9VSA21-00486-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno.

Recomendamos a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos	Tipo de malware	Documento web
2b41b43a834b2478d5847e662c060b21e3a4a379f2b474b7dc14b1fd5c4eeefb	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
4473e22ad40e816cd3d172e45e06dbf5b7efb3fd3f7ea1c23e786051cad5756a	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
f0e1abf821003b21880756b6697a96e818031a94653815f09869f29c704608da	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
90786a6e788d4541051f2c754fc6b9dd803197de775959f7e76b67c02876c7d8	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
0945ad2b9a16c4cee10805425ab4270095739f8f993e5b4a68730876fc60bd72	MSIL/Kryptik.ABOX!tr	2CMV21-00200-01
00de32152d8bbc2f8b7c455964234418ef535750d11af0af3a5c7138274b6de2	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
35e1132c4d5bd6ce3bb574fb61d0da63e98f3b473c72052c218cfa7d8927750a	MSIL/Kryptik.ABOX!tr	2CMV21-00200-01
b18f41f963af2064d1cf3101631a1ae7426dfb327bfe6756b0d7cf16f7ebdd35	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
222c5cbdc358ef41c0493d1f656a759e4dc0c7635148833901924490b43581db	MSIL/Kryptik.ABOX!tr	2CMV21-00200-01
b0871e4ff17df03f7513bf5ed9aed71d6011c6542b3016324b4a15743f69d05b	MSIL/Kryptik.ABSG!tr	2CMV21-00200-01
4189b55247d620166ed58da46949e5a4227c82748364fc61cd06ac83e8219417	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
c44d428719c6f94f419fc91704c34bf27909d1daffee1baa17f97d873d3d46a4	HTML/MsPhishing.4231!tr	2CMV21-00200-01
e913d86e60cb4ac0e0008015a78c78d780f5f210bb410e06fcded6fa0a22bc2b	HTML/MsPhishing.4231!tr	2CMV21-00200-01
22a4bd616aa1cc32e51344ca9ccaba7fc38608ddd8e73ef7557ba05ed65d9008	HTML/Phish.70A6!phish	2CMV21-00200-01
98baffb5cd3cda0c33648f487a7185a258589067b1f49adbc1d484032f6e95f5	HTML/Phish.70A6!phish	2CMV21-00200-01
a9cc8cddb4c92d03e27ded9f766597de8d763bf537029b487952f43f3f7f837c	W32/Kryptik.EPLE!tr	2CMV21-00200-01
71e3eb82dc3b703a8dba3b4d98b38485edf4ff8711b0cee42c9688323f7d6bb8	Malicious_Behavior.SB	2CMV21-00200-01

1920fa7022ce82e956bef779d31f34e96c1a55769797545e55f8da8d093b671d	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01
a9f12b56f2057a88ccf7e9424fd158072e2ade913c2224c3c1106ea487449024	MSIL/Kryptik.ABOX!tr	2CMV21-00200-01
d2782bda4b66e405aa6d987623f964aa1cc974cc134a63c964be47e53b473052	MSIL/Kryptik.ABOX!tr	2CMV21-00200-01
3cea6bd93b9412c8b37dcddf638ee4a4c8a903fc6072fb14d72c0297bafd212e	MSIL/Kryptik.ABQV!tr	2CMV21-00200-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

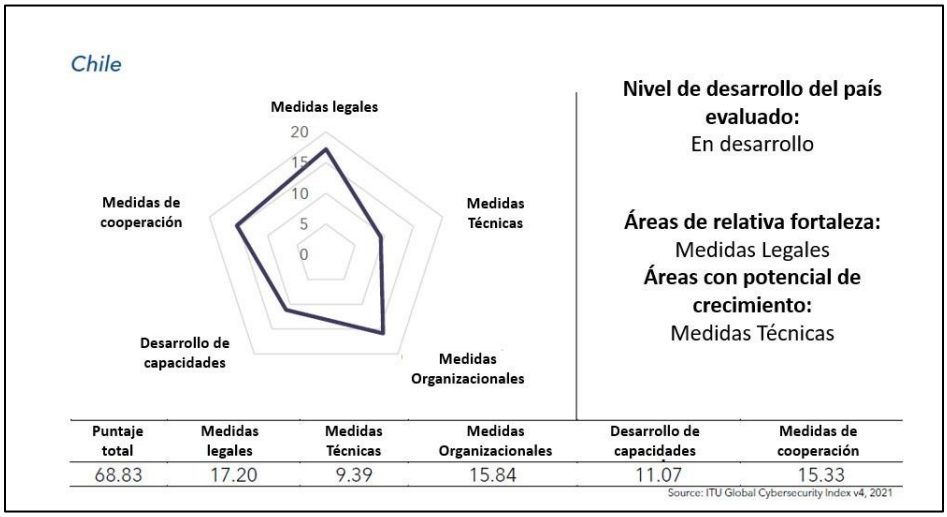
IP	Etiqueta de sistema autónomo	Documento web
103.232.55.10	VietServer Services technology company limited	2CMV21-00200-01
198.251.79.80	1&1 Ionos Se	2CMV21-00200-01
103.155.82.221	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00200-01
209.97.145.73	DIGITALOCEAN-ASN	2CMV21-00200-01
81.21.172.152	Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.	2CMV21-00200-01
103.167.84.243	VietServer Services technology company limited	2CMV21-00200-01
192.185.46.187	UNIFIEDLAYER-AS-1	2CMV21-00200-01
159.89.122.235	DIGITALOCEAN-ASN	2CMV21-00200-01
86.122.125.173	RCS & RDS	2CMV21-00200-01
165.227.27.58	DIGITALOCEAN-ASN	2CMV21-00200-01
45.137.22.39	RootLayer Web Services Ltd.	2CMV21-00200-01
66.154.111.172	PERFORMIVE	2CMV21-00200-01
185.222.58.116	RootLayer Web Services Ltd.	2CMV21-00200-01

Actualidad

CiberSucesos No. 11 | Secuestro de Whatsapp y SIM swapping

Dedicamos el undécimo número de CiberSucesos a las amenazas que se centran en nuestros celulares, como el secuestro de SIM card y el robo de las cuentas de Whatsapp, además de malware que apuntan a los smartphones. Conoce más aquí: https://csirt.gob.cl/recomendaciones/cibersucesos-no-11-secuestro-de-whatsapp-y-sim-swapping/.

Chile avanza nueve puestos a nivel mundial y dos en América en ranking global de ciberseguridad de la ONU



En la cuarta edición del prestigioso ranking de ciberseguridad mundial Global Cybersecurity Index, desarrollado por la Unión Internacional de Telecomunicaciones (ITU, agencia de las Naciones Unidas especializada en la coordinación de las telecomunicaciones a nivel global), el cual refleja los avances logrados en materia de ciberseguridad por los 194 estados miembros y presentado hoy, **Chile subió nueve lugares a nivel mundial, llegando al puesto 74, y dos en términos del continente americano, ubicándose séptimo en la región**.

El Subsecretario del Interior, Juan Francisco Galli, destaca reconocimiento del avance de nuestro país en la protección del ciberespacio, aunque llama a mantener e intensificar la concientización de la ciudadanía en la adopción de prácticas seguras en internet.

Nuestro puesto en este listado internacional deberá mejorar aún más el próximo año, con la creación de la Agencia Nacional de Ciberseguridad. La noticia completa, pueden leerla en el siguiente enlace: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-denuncia-sitio-de-notaria-falsa-para-que-sea-dado-de-baja/.

Últimos cupos para participar del OEA Cyberwomen Challenge Chile 2021 este 8 de julio

Este jueves 8 de julio comienza el OEA Cyberwomen Challenge Chile, competencia de hacking entre equipos conformados solo por mujeres. El evento, organizado desde el año 2018 por el CSIRT de Gobierno del Ministerio del Interior y la Organización de Estados Americanos (OEA) en alianza junto a TrendMicro, se desarrolla en 10 países de Latinoamérica: Colombia, Guatemala, México, Uruguay, Perú, República Dominicana, Argentina, Brasil, Costa Rica y Chile.

El Cyberwomen Challenge nace con el objetivo de potenciar a las mujeres en una industria donde existe una baja tasa de ocupación femenina (en 2020 sólo un 25% de los puestos de trabajo en ciberseguridad a nivel global eran ocupados por mujeres). Para ello, se creó esta instancia anual, donde cientos de mujeres con interés y habilidades en la ciberseguridad puedan conocerse, generar contactos y demostrar sus capacidades.

En nuestro país y desde 2018, ya han participado en el Cyberwomen Challenge más de 300 mujeres de distintas edades y carreras. El evento de Chile, como aquellos en sus pares de la región, es clasificatorio para el OEA Cyberwomen Regional, a realizarse en 2022.

La inscripción se realiza en el siguiente sitio web oficial y aún quedan los últimos cupos para participar: https://women-challenge.interior.gob.cl

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- Francisco Javier Ortega Ferias
- iu-friend
- Juan Andrés Huechan Marilef
- Mackarena Vicencio Rojas
- Alejandra Carolina Gutiérrez Castillo
- Jaime Araya Aros
- Guillermo Correa Martínez
- Daniela Gajardo
- José Ossa Monge
- Andrés Reyes
- Manuel Varela Mancilla
- Alex Orellana Rivera

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.02 16:30:38 -04'00'