Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

18-06-2021 | Año 3 | N°102

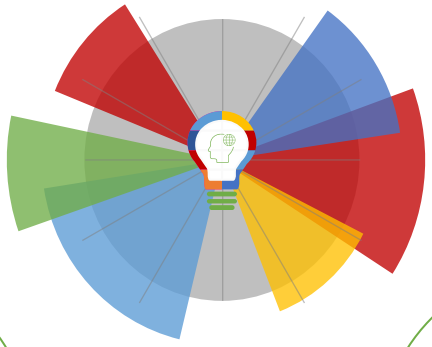
Boletín de Seguridad Cibernética

Semana del 11 al 17 de junio de 2021

La semana en cifras

Hash
2
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
19
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
29
para vulnerabilidades
Las mitigaciones son útiles en productos de Apple, Cisco y Google.

IP
17
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

Imagen del mensaje

CSIRT alerta ante campaña de malware que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00193-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de junio de 2021
Última revisión	16 de junio de 2021
Indicadores de compromiso	
SHA256	
ED2BC65531659CBFB937975F088D2560E741BAF4001EEBE44065E9254BADE683 0097E775B3ED33D109E970472D5F8FD5D76CAA2D28E42419BC2C8154033649AF	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00193-01/	
https://csirt.gob.cl/media/2021/06/2CMV21-00193-01.pdf	

Sitios fraudulentos

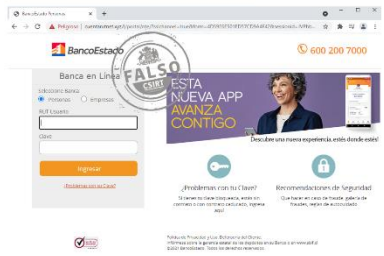
CSIRT advierte de página fraudulenta que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR21-00962-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2021
Última revisión	11 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://hintek[.]cl/.storage/htpasswds/login.php	
IP	
[201.148.104.135]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00962-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00962-01.pdf	

CSIRT advierte de sitio fraudulento que suplanta a Amazon	
Alerta de seguridad cibernética	8FFR21-00963-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2021
Última revisión	11 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://lordandpost[.]info/clamz/	
IP	
[207.174.214.152]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00963-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00963-01.pdf	

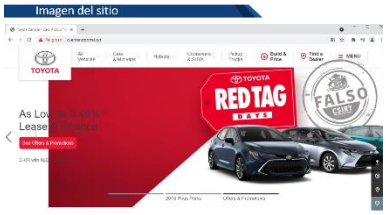
Imagen del sitio

CSIRT advierte de sitio fraudulento que suplanta a Office365 y Outlook	
Alerta de seguridad cibernética	8FFR21-00964-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2021
Última revisión	11 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://chileanylgroup[.]cl/wp-admin/documentview/	
IP	
[66.165.231.114]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00964-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00964-01.pdf	

Imagen del sitio



CSIRT advierte de sitio fraudulento que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR21-00965-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2021
Última revisión	14 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://cuentarutnet[.]xyz/	
IP	
[142.11.210.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00965-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00965-01.pdf	



CSIRT alerta ante sitio fraudulento que suplanta a Toyota	
Alerta de seguridad cibernética	8FFR21-00966-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2021
Última revisión	14 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://cuentarutportal[.]xyz/	
IP	
[142.11.210.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00966-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00966-01.pdf	

CSIRT advierte ante sitio fraudulento que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR21-00967-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2021
Última revisión	14 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://unibac.edu[.]co/Clientes/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[162.214.171.224]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00967-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00967-01.pdf	

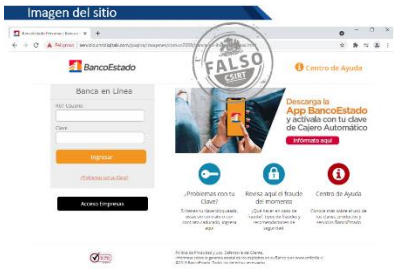
Imagen del sitio		
	**CSIRT advierte ante sitio fraudulento que suplanta al BancoEstado**	
	Alerta de seguridad cibernética	8FFR21-00968-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	14 de junio de 2021
	Última revisión	14 de junio de 2021
	Indicadores de compromiso	
	URL sitio falso	
	https://servicio.cnndigitals[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html	
	IP	
	[54.39.173.96]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr21-00968-01/	
	https://www.csirt.gob.cl/media/2021/06/8FFR21-00968-01.pdf	

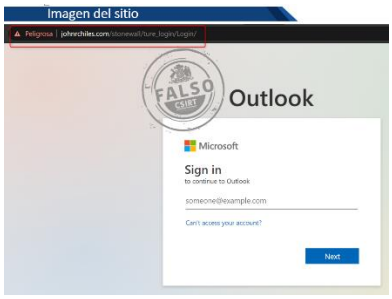
Imagen del sitio		
	**CSIRT advierte ante sitio fraudulento que suplanta al Banco Santander**	
	Alerta de seguridad cibernética	8FFR21-00969-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	14 de junio de 2021
	Última revisión	14 de junio de 2021
	Indicadores de compromiso	
	URL sitio falso	
	https://bancc-santandr.cl-hsp[.]xyz/16236829O5/index.asp	
	IP	
	[104.21.80.253]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr21-00969-01/	
	https://www.csirt.gob.cl/media/2021/06/8FFR21-00969-01.pdf	

Imagen del sitio

CSIRT advierte de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00970-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2021
Última revisión	14 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://checksms-app[.]website/1623682933/personas/index.asp	
IP	
[199.188.201.122]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00970-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00970-01.pdf	

Imagen del sitio

CSIRT advierte ante sitio fraudulento que suplanta a Colloky	
Alerta de seguridad cibernética	8FFR21-00971-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2021
Última revisión	15 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://www.colokinfantil[.]online/my_account.html	
IP	
[5.255.62.132]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00971-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00971-01.pdf	



CSIRT advierte ante sitio fraudulento que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR21-00972-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de junio de 2021
Última revisión	16 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://johnrchiles[.]com/stonewall/ture_login/Login/	
IP	
[69.49.234.241]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00972-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00972-01.pdf	

CSIRT advierte ante sitio fraudulento que suplanta a Wells Fargo	
Alerta de seguridad cibernética	8FFR21-00973-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://johnrchiles[.]com/stonewall/ture_login/Login/	
IP	
[69.49.234.241]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00973-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00973-01.pdf	

CSIRT alerta de página fraudulenta que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR21-00974-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
http://bitalchile[.]cl/	
IP	
[186.64.118.115]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00974-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00974-01.pdf	

Phishing

CSIRT advierte campaña de phishing que suplanta a Microsoft Outlook web	
Alerta de seguridad cibernética	8FPH21-00408-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2021
Última revisión	11 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://tyyyyyyy.000webhostapp[.]com/it/admin/	
IP	
[145.14.144.213]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00408-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00408-01.pdf	

CSIRT alerta por campaña de phishing que extorsiona con supuestas fotos comprometedoras	
Alerta de seguridad cibernética	8FPH21-00409-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2021
Última revisión	14 de junio de 2021
Indicadores de compromiso	
Servidor SMTP	
[181.118.46.149]	
[78.30.10.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00409-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00409-01.pdf	

CSIRT advierte ante campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00410-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2021
Última revisión	15 de junio de 2021
Indicadores de compromiso	
URL sitio redirección	
https://bit[.]ly/2RVayFN?l=www.bancoripley.cl	
https://kukul[.]mx/wp-content/languages/plugins/enviar02.php?l=494638175	
https://bit[.]ly/35khi2Z?l=www.bancoripley.cl	
hxxp://185.8.129.126/activacion/cuenta-bwng/	
URL sitio falso	
http://www-bancoripleycl.rbsystems[.]lt/login	
IP	
[5.20.67.27]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00410-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00410-01.pdf	

Vulnerabilidades

CSIRT alerta por vulnerabilidades críticas en productos de Apple	
Alerta de seguridad cibernética	9VSA21-00455-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2021
Última revisión	15 de junio de 2021

CVE		
CVE-2021-30761	CVE-2021-1871	CVE-2021-30663
CVE-2021-30762	CVE-2021-1879	CVE-2021-30665
CVE-2021-1782	CVE-2021-30657	CVE-2021-30666
CVE-2021-1870	CVE-2021-30661	CVE-2021-30713

Fabricante
Apple

Productos afectados
iOS 12.5.3
iPhone 5s
iPhone 6
iPhone 6 Plus
iPad Air
iPad mini 2
iPad mini 3
iPod touch

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00455-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00455-01.pdf

CSIRT alerta ante vulnerabilidades graves en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00456-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio de 2021

CVE		
CVE-2021-1242	CVE-2021-1524	CVE-2021-1543
CVE-2021-1568	CVE-2021-1567	CVE-2021-1571
CVE-2021-1395	CVE-2021-1541	CVE-2021-1134
CVE-2021-1569	CVE-2021-1542	CVE-2021-1566
CVE-2021-1570		

Fabricante
Cisco

Productos afectados
Cisco AnyConnect Secure Mobility
Cisco Jabber
Cisco Webex
Cisco AnyConnect
Cisco Unified Intelligence Center
Cisco Meeting Server API
Cisco Small Business 220 Series Smart Switches
Cisco DNA Center Software
Cisco Email Security Appliance
Cisco Web Security Appliance

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00456-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00456-01.pdf

CSIRT advierte de vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00456-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio de 2021

CVE	
CVE-2021-30554	CVE-2021-30556
CVE-2021-30555	CVE-2021-30557

Fabricante
Google

Productos afectados
Google Chrome: 89.0.4389.72 a 91.0.4472.101.

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00457-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00457-01.pdf

Actualidad

Comienzan inscripciones al OEA Cyberwomen Challenge Chile 2021, competencia para mujeres con habilidades en ciberseguridad

Este martes 15 de junio comenzaron las inscripciones para la fase en Chile del cuarto OEA Cyberwomen Challenge, competencia de hacking entre equipos conformados solo por mujeres que tendrá lugar el 8 de julio. 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.

La inscripción se realiza en el siguiente sitio web oficial: https://women-challenge.interior.gob.cl/.

Como parte de la promoción del Cyberwomen Challenge Chile 2021, altas autoridades han decidido acompañarnos con un video apoyando la convocatoria. Pueden encontrarlos aquí:

Ministra de la Mujer y Equidad de Género Mónica Zalaquett: youtube.com/watch?v=UTOJ81bJRd8

Subsecretaria de Ciencia Carolina Torrealba: https://www.youtube.com/watch?v=_pX5zVXhF_I

Ministro del Interior Rodrigo Delgado: https://www.youtube.com/watch?v=cm9P5esveFI

Subsecretario del Interior Juan Francisco Galli: https://www.youtube.com/watch?v=yhfOs0tpnUQ

Cómic | Benkid, pro gamer 147

¿Cómo pueden los padres enseñar a tus hijos los riesgos de los juegos online? Para evitar que los menores caigan en peligros como el grooming, elaboramos este didáctico comic para facilitar el instruir a los hijos sobre lo necesario para cuidarse al jugar en línea. Encuéntralo aquí: csirt.gob.cl/recomendaciones/comic-benkid-pro-gamer-147/.

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.

- Marco
- Carlos Retamales
- Pablo Ignacio Araya del Pino
- Hanz Sandoval
- Camilo Esteban Orellana Diaz
- Juan Luis Adasme Troncoso
- iufriend

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.18 15:29:28 -04'00'