27.08-2020 | Año 2 | N°60

Boletín de Seguridad Cibernética

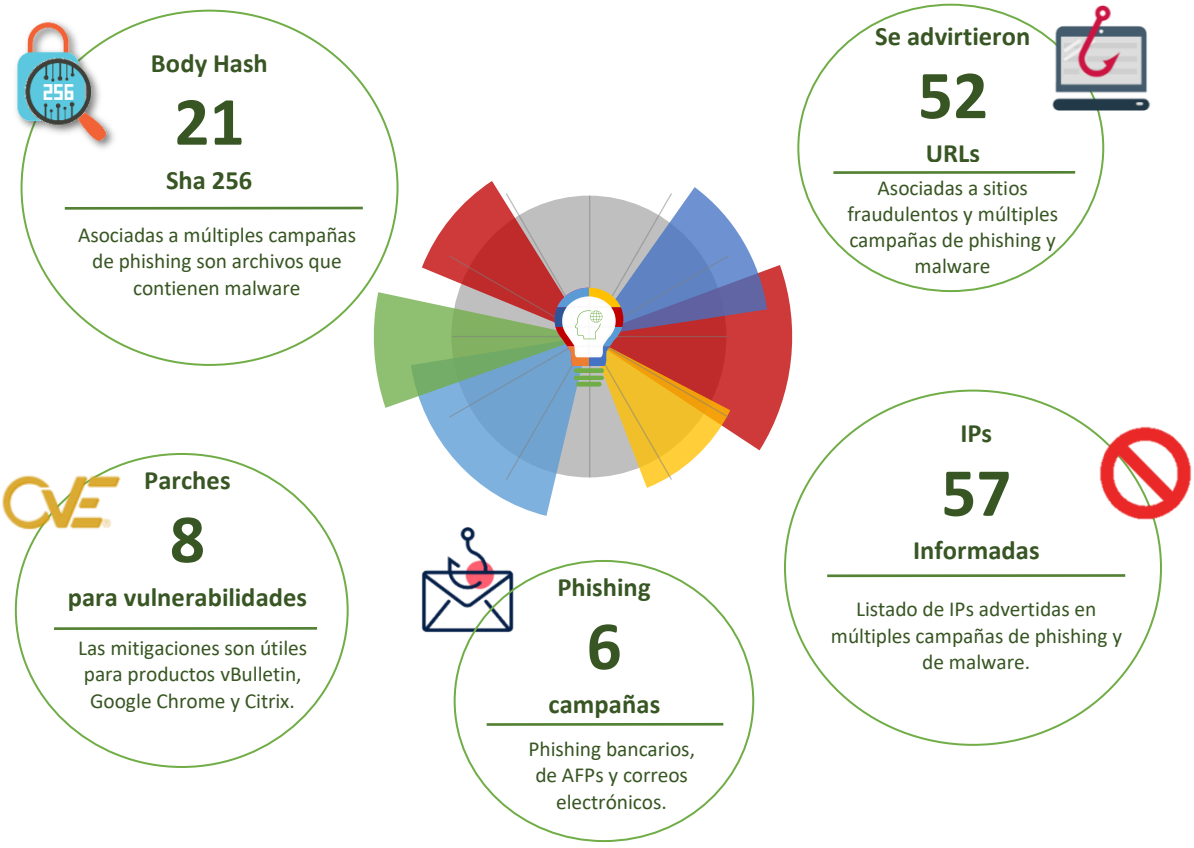
Semana del 20 al 26 de agosto de 2020

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Resumen de la semana en cifras



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

Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte web que suplanta sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00630-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
cpbild[.]co/netflix~11746	
IP	
99[.]84[.]174[.]99	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00630-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00630-01.pdf	

Imagen del sitio

CSIRT informa de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00631-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-login[.]link/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
199[.]188[.]200[.]199	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00631-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00631-01.pdf	

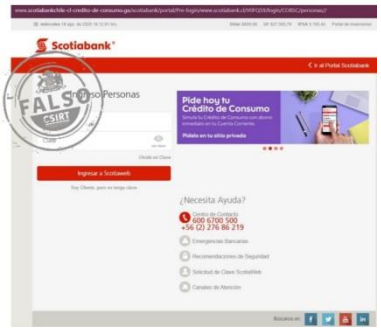
Imagen del sitio

CSIRT advierte de sitio que suplanta web de servicio de streaming	
Alerta de seguridad cibernética	8FFR20-00632-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
netflix-loign[.]auth[.]service-id[.]com[.]supersindicoprofissional[.]com	
IP	
107[.]161[.]182[.]91	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00632-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00632-01.pdf	

Imagen del sitio

CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00633-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
linier[.]com[.]br/www[.]santander[.]cl/pagina/login[.]asp	
IP	
187[.]17[.]111[.]35	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00633-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00633-01.pdf	

Imagen del sitio

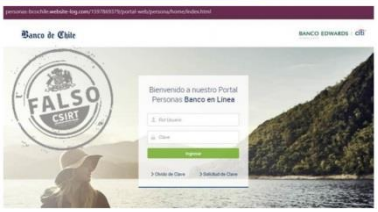


CSIRT advierte de portal que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00634-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-credito-de-consumo[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00634-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00634-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00635-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-credito-personal[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00635-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00635-01.pdf	

Imagen del sitio



CSIRT informa sobre sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00636-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
personas-bcochile[.]website-log[.]com	
IP	
208[.]73[.]200[.]206	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00636-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00636-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00637-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
dbesoluciones[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
204[.]93[.]183[.]55	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00637-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00637-01.pdf	

Imagen del sitio

CSIRT informa de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00638-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
netflixaccounts2022[.]tk	
IP	
172[.]217[.]214[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00638-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00638-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00639-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-credito-personales[.]cf/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00639-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00639-01.pdf	

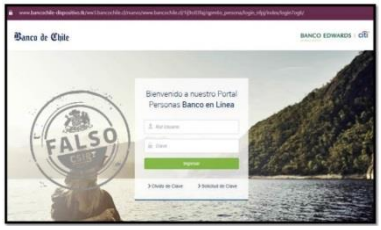
Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00640-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
empresas-bancoestado[.]link	
IP	
68[.]65[.]123[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00640-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00640-01.pdf	

Imagen del sitio

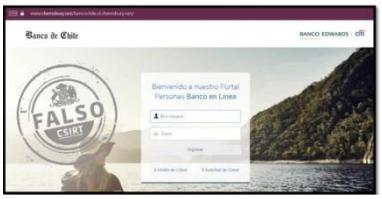
CSIRT informa sobre sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00641-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-dispositivo[.]tk/scotiabank/portal/Pre-login/www.scotiabank.cl/OK3V8V/login/AKPWW/personas//	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00641-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00641-01.pdf	

Imagen del sitio



CSIRT advierte sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00642-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Agosto de 2020
Última revisión	22 de Agosto de 2020
Indicadores de compromiso	
URL	
www[.]bancochile-dispositivo[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00642-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00642-01.pdf	

Imagen del sitio



CSIRT informa de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00643-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Agosto de 2020
Última revisión	22 de Agosto de 2020
Indicadores de compromiso	
URL	
www[.]chemsbury[.]net/bancochile[.]cl[.]chemsbury[.]net/	
IP	
43[.]255[.]154[.]37	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00643-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00643-01.pdf	

Imagen del sitio

CSIRT informa de portal de streaming fraudulento	
Alerta de seguridad cibernética	8FFR20-00644-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Agosto de 2020
Última revisión	22 de Agosto de 2020
Indicadores de compromiso	
URL	
my-netflix[.]tk	
IP	
108[.]177[.]112[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00644-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00644-01.pdf	

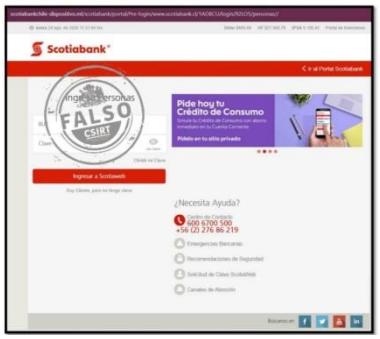
Imagen del sitio

CSIRT advierte de suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00645-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Agosto de 2020
Última revisión	22 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://bestadiosms[.]verifyw[.]website/?afp=1	
IP	
192[.]64[.]118[.]39	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00645-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00645-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00646-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Agosto de 2020
Última revisión	25 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-credito-de-consumo[.]gq	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00646-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00646-01.pdf	

Imagen del sitio



CSIRT informa de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00647-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-dispositivo[.]ml	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00647-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00647-01.pdf	

Imagen del sitio

CSIRT advierte de falso portal para fraudes bancarios	
Alerta de seguridad cibernética	8FFR20-00648-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bit[.]do/bancoestadoseguridad	
bancoestadocl[.]link/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]54[.]116[.]17	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00648-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00648-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00649-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bit[.]do/santandermovil	
banco-santande-r[.]link	
IP	
198[.]54[.]115[.]164	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00649-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00649-01.pdf	

CSIRT advierte sobre sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00650-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://bchile-areasegura[.]website/?segu=1	
chilebanc-seguridadzona[.]website	
IP	
199[.]188[.]200[.]12	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00650-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00650-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00651-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bestarreda[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
62[.]149[.]128[.]151	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00651-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00651-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00652-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Agosto de 2020
Última revisión	18 de Agosto de 2020
Indicadores de compromiso	
URL	
acceso-falabella-cl[.]info	
IP	
134[.]209[.]107[.]191	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00652-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00652-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00653-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]vipaelettronica[.]it/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
151[.]80[.]80[.]206	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00653-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00653-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00654-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-consumos[.]gq	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00654-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00654-01.pdf	

Imagen del sitio

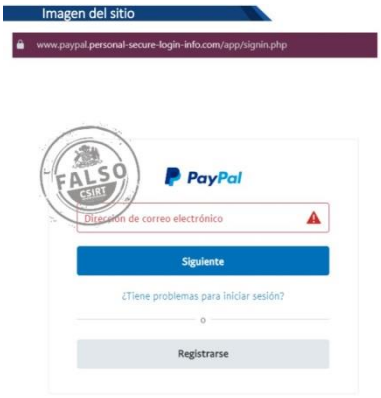
CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00655-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bci[.]enlinea[.]cbl-chile[.]info	
IP	
159[.]89[.]165[.]229	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00655-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00655-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00656-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bit[.]do/bancoestado-personas	
bancoestado-personas[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
159[.]89[.]165[.]229	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00656-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00656-01.pdf	

Imagen del sitio

CSIRT advierte sobre web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00657-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-cl-chile-portal[.]cf/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00657-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00657-01.pdf	



CSIRT advierte sobre sitio que suplanta portal de pago	
Alerta de seguridad cibernética	8FFR20-00658-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
paypal[.]personal-secure-login-info[.]com/app/signin[.]php	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00657-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00657-01.pdf	

Phishing

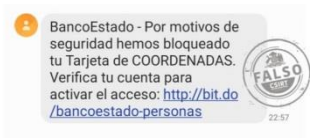
Imagen del mensaje

CSIRT advierte de phishing de empresa de correos	
Alerta de seguridad cibernética	8FPH20-00297-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://www.mrknowledgecity[.]org/logo/fedex/7zwzbxr6f4k5gc5pl20d0ep227524e5d5582cfb0ee5b91de81c038c5.php?email=	
IP	
[210.152.127.28]	
[119.18.54.40]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00297-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00297-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por saturación de correo	
Alerta de seguridad cibernética	8FPH20-00298-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps[:]//fragoimpex[.]com/secolvwmm6xn5q28snfaasni[.]php	
IP	
[41.190.32.15]	
74.124.217.48	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00298-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00298-01.pdf	

Imagen del mensaje



CSIRT advierte smishing por bloqueo en tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00299-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxp://bit[.]do/bancoestado-personas	
hxxps://bancoestado-bancaporinternet[.]link/imagenes/comun2008/banca-en-linea-personas.html?id=2978e0c34dbebfc46bf96c994436a5790a22017a&cat=login.secure&gClic=5c04925674920eb58467fb52ce4ef728&valueValidar&q=true	
IP	
68.65.123.126	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00299-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00299-01.pdf	

Imagen del mensaje

CSIRT advierte campaña de phishing por clave caducada	
Alerta de seguridad cibernética	8FPH20-00300-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxp://schafoga[.]com/cliente/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.123.240]	
[45.236.130.118]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00300-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00300-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por transferencia retenida	
Alerta de seguridad cibernética	8FPH20-00301-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
http://zimaamag.com/scos.php	
hxxps://scotiabankchile-cl-consumos[.]gq/scotiabank/portal/Pre-login/	
IP	
[103.248.146.11]	
[91.234.99.119]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00301-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00301-01.pdf	

Imagen del mensaje

CSIRT informa sobre phishing por problemas en cuenta de streaming	
Alerta de seguridad cibernética	8FPH20-00302-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Agosto de 2020
Última revisión	26 de Agosto de 2020
Indicadores de compromiso	
URL	
https://gappingfarmound.blogspot.com/	
hxxp://a0465455.xsph[.]ru/laz/users/userID-51954/myaccount/home.php	
IP	
[58.159.206.58]	
[141.8.192.58]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00302-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00302-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones obtenidas de Jenkins	
Alerta de seguridad cibernética	9VSA20-00287-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2020
Última revisión	20 de Agosto de 2020
CVE	
CVE-2019-17638	
Fabricante	
Jenkins	
Productos afectados	
Jenkins weekly versión 2.242 y anteriores. Jenkins LTS versión 2.235.4 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00287-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00287-01.pdf	

CSIRT comparte actualizaciones obtenidas de Google	
Alerta de seguridad cibernética	9VSA20-00288-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
CVE	
CVE-2020-6556	
Fabricante	
Google	
Productos afectados	
Versiones anteriores a la 84.0.4147.135 para Windows, Mac y Linux.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00288-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00288-01.pdf	

CSIRT comparte información sobre una vulnerabilidad obtenida de Haxx	
Alerta de seguridad cibernética	9VSA20-00289-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
CVE	
CVE-2020-8231	
Fabricante	
Haxx	
Productos afectados	
Las versiones afectadas son libcurl desde la versión 7.29.0 hasta la 7.71.1 (incluida).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00289-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00289-01.pdf	

CSIRT comparte actualización obtenida de Wireshark	
Alerta de seguridad cibernética	9VSA20-00290-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2020
Última revisión	21 de Agosto de 2020
CVE	
CVE-2020-17498	
Fabricante	
Wireshark	
Productos afectados	
Wireshark desde la versión 3.2.0 hasta la 3.2.5 (incluida).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00290-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00290-01.pdf	

CSIRT comparte actualizaciones obtenidas de PostgreSQL	
Alerta de seguridad cibernética	9VSA20-00291-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Agosto de 2020
Última revisión	24 de Agosto de 2020
CVE	
CVE-2020-14349 - CVE-2020-14350	
Fabricante	
PostgreSQL	
Productos afectados	
PostgreSQL desde la versión 10 hasta la 12.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00291-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00291-01.pdf	

CSIRT comparte actualizaciones obtenidas de VMWare	
Alerta de seguridad cibernética	9VSA20-00292-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Agosto de 2020
Última revisión	24 de Agosto de 2020
CVE	
CVE-2020-3976 - CVE-2020-3975	
Fabricante	
VMWare	
Productos afectados	
ESXi versiones 7.0, 6.7 y 6.5. Cloud Foundation (ESXi) versiones 4.x.x y 3.x.x. vCenter Server versiones 7.0, 6.7 y 6.5. Cloud Foundation (vCenter) versiones 4.x.x y 3.x.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00292-01/	
https://www.csirt.gob.cl/media/2020/08/9VSA20-00292-02.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad.

CSIRT recomienda 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 reportados. Recomendación: bloquear
0192c3a7269dfdc793006d589bda8096879680abb59bfc823e6edaf2baeeb41e
042c1f08577aeeebdbfb0213c9abf91cf3760213483dd1575a19e9f255417962
04ed313f0c28c0f07e054a223bcce3991932e313f7c233013dcd6e2f945f9f80
178fe3c3f021fd3abe778a9342d10d458b4b1a5d8da37736c9f8d5bf0b75f3fb
1e55fae2ce547704d03125badc64d0943f64c4b133ecad738ac192670caf6db4
464ceb8b017cbf2e01dd6666d6696458873ddedd0b5159f464fae8e680f0716c
522ea0351bf4ae37fb68315f5ef7cfeaf2cfc83897311a4b61e9247b85ac163d
575f76694922593e0710e6558c3bc3659773a01676a7bb85b834d41b6fbc0303
703840048b7c7bab387e1af771fbb2dc848713fd97bff6e5136d9416a8886a0d
850446be6e5713cc5f6059d9453cb332fdd6b6ef86a682e69eca3c36744d54ac
8ccefd02988cad2fe86336a83e4fccac4e0519550cc4b11061bba50dd09bcd14
9d0e5ae7e5a447017bb5044faa300f671825d01997042d81fa65e12d292fca38
9f82a6df32123ef98e8cc6c4c7aba91436d6aa87ce5eb9728348d1bfd48b9fb5
af72b92635b18607f5affdb190646a49fcfb3b980e979774c2084b1b9ba4f205
b30445e7baf6935ed806d230f1587bd810ea43c5bb8ff6623fa18d8f7b86fb0c
b4ade69aff5e1ed84fb38bba4cfba617516206037 38b6859d5e9e69895c18e0f
c83264bbb5b4dfc1bd60b805ddedb9e4ee7344a3e79266b3a30019453d8cfd2a
e45112e3caca712cebfd264c5549b378fac2e3f89a30c615fb4a43a747377037
e7eb9296ed7a22e6ad9048ec60ff569cb899440fc4ed72cca7e3a1e166f6aebd
ecde1cde56fd892bda63f653a4c2a74ef3a1e36adfe503d7e1df3f9ffd3c8bf5
f0d838a88e4a5e186e34a953219c7378cf8486efa7b5c1d04511f4f4c83fa561

Archivos reportados. Recomendación: mantener en observación
41.203.14.180
45.137.22.37
88.218.16.194
209.50.52.217

185.99.235.86
61.4.79.11
45.137.22.146
45.147.231.33
95.211.253.201
210.59.136.112
195.78.94.202
103.247.10.74
196.41.213.18
197.220.196.20
41.203.14.180
212.66.109.106
61.4.79.11

Correo electrónico. Observación: mantener en observación
alessandro.desimoni@bcccollialbani.it
ali.alzoubaidi@trust.com.jo
aosk.t@nicouae.com
atendimento5@balarotidesign.com.br
Charity.Madenyika@methodist.org.uk
cnexus@nexusship.com
comercial@focalteccr.com
doryyaz38@yahoo.com
fanll@npsel.com
Helen.Xie@futuralimited.com
jm@rochecouste.co.za
jmtc.import@jaipur.ae
kiku@vissel.com.tw
oceanwin@ytp.com.mm
press@nexushub.co.za
rosane@lightecon.com.br
rud-division@acgbahamas.com
rudy.josano@ptsjpl.com
Solicitors@hgc.com
spares@vw-tirupati.co.in
support@dhl.com

URL. Recomendación: mantener en observación
hxxp://hapaistanbul[.]com/tweHyPvH/
hxxp://hcsnet[.]com[.]br/QIn7l26597670/
hxxp://krabitourtransfer[.]com/WLdPbPn/
hxxp://kravmagaireland[.]com/cgi-bin/X5h427139317/
hxxp://labonni[.]com[.]br/pCG/
https://6iptv[.]com/urc8d69/KjvTNZzN/
hxxp://san-jose-roofing[.]com/cpgmz/AcdMcVRS/
hxxp://websender[.]org/wp-admin/BiyKnfrTY/
hxxp://avenueleaseandrentals[.]com/plugins/a83E826dz6s6205/
hxxp://agtrade[.]hu/images/GEwrjxo8p85338/

Recomendaciones y Buenas Prácticas

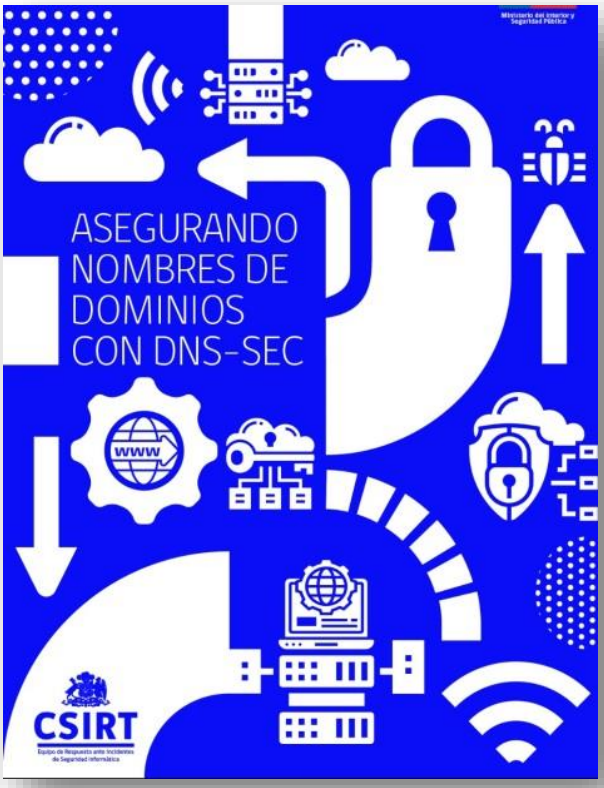
Recomendaciones generales de seguridad

- 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.

Investigación

Asegurando Nombres de Dominios con DNSSEC

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la décimo quinta edición de su publicación sobre amenazas cibernéticas el que analiza la seguridad en DNS a través de la implementación de DNSSEC. El artículo fue elaborado por Benjamin Aravena y Carlos Landeros.
El trabajo hace hincapié en las amenazas, especialmente en perspectiva de las mejoras que ofrece DNSSEC, identificando algunas de ellas, como el envenenamiento del caché y la falsificación de registros. Posteriormente explica cómo es el funcionamiento de DNSSEC al ser implementado y finalmente da cuenta de los beneficios del mismo, el rol que juega como parte del concepto general de seguridad del DNS y la implementación del caso en la Red de Conectividad del Estado, el que permite asegurar a los dominios de muchos servicios públicos frente a diversas amenazas y riesgos de internet.



Ver más en: https://www.csirt.gob.cl/reportes/an2-2020-15/

Actualidad

El sexting es una práctica voluntaria que cada día va tomando más adeptos, incluso en los adolescentes. El problema es que el compartir imágenes con contenido sexual puede derivar en distintos riesgos, como por ejemplo, acoso sexual o que la publicación llegue a malas manos. Para prevenir, lo fundamental es educar y guiar a los hijos desde chicos.

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

- Jorge Moraga
- Gabriel Iruasquin
- Matia Cornejo

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.08.28 20:24:59 -04'00'