01-10-2020 | Año 2 | N°65

Boletín de Seguridad Cibernética

Semana del 24 al 30 de Septiembre 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

Body Hash

32

Sha 256

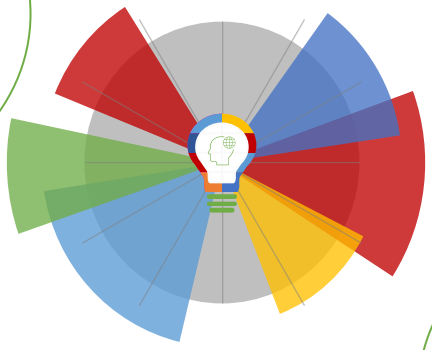
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron

75

URLs

Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches

6

para vulnerabilidades

Las mitigaciones son útiles para productos Cisco.

IPs

55

Informadas

Listado de IPs advertidas en múltiples campañas de phishing y de malware.

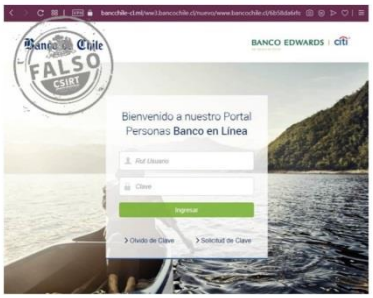
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl

Contenido

Sitios fraudulentos 3
Phishing 20
Indicadores de Compromisos 21
Recomendaciones y Buenas Prácticas 25
Muro de la Fama 26

Sitios fraudulentos

Imagen del sitio

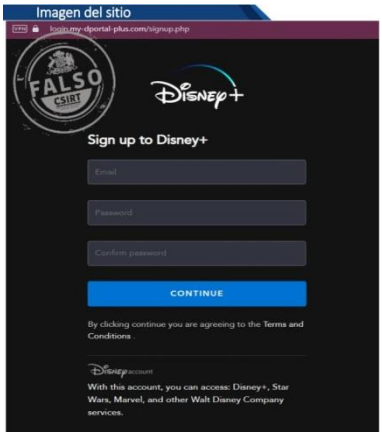


CSIRT informa de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00732-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancchile-cl[.]ml	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00732-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00732-01.pdf	

Imagen del sitio

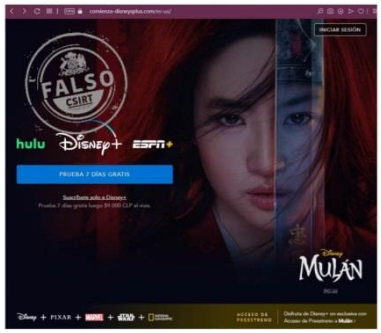
CSIRT advierte sobre sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00733-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchle-dispositivo[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00733-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00733-01.pdf	

Imagen del sitio



CSIRT advierte sobre web de suplantación de sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00734-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
login[.]my-dportal-plus[.]com/signup[.]php	
IP	
185[.]82[.]127[.]52	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00734-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00734-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de streaming falso	
Alerta de seguridad cibernética	8FFR20-00735-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
comienza-disneysplus[.]com	
IP	
45[.]32[.]125[.]197	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00735-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00735-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00736-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
banchille-aumento-cupo[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00736-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00736-01.pdf	

Imagen del sitio

CSIRT advierte de web de suplantación de portal bancario	
Alerta de seguridad cibernética	8FFR20-00737-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
aumento-banchile[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00737-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00737-01.pdf	

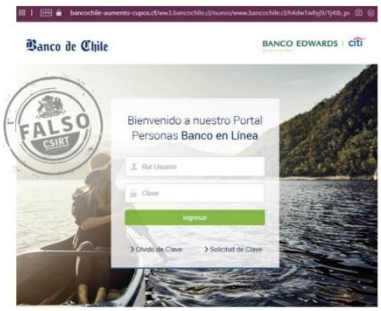
Imagen del sitio

CSIRT informa sobre portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00738-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
banchille-aumento-cupo[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00738-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00738-01.pdf	

Imagen del sitio

CSIRT advierte sobre falso portal de streaming	
Alerta de seguridad cibernética	8FFR20-00739-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
us-netftix[.]com/app/login[.]php	
IP	
45[.]133[.]200[.]3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00739-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00739-01.pdf	

Imagen del sitio

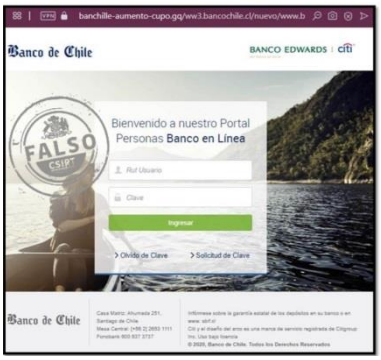


CSIRT advierte de web que suplanta sitio bancario	
Alerta de seguridad cibernética	8FFR20-00740-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancochile-aumento-cupos[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00740-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00740-01.pdf	

Imagen del sitio

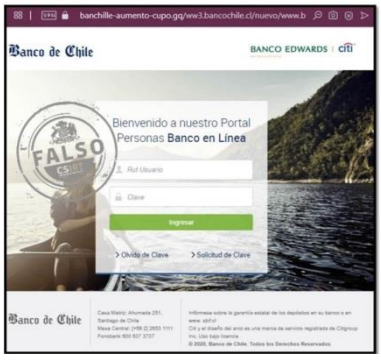
CSIRT informa de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00741-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://sms-santder[.]website/?sms=1	
IP	
162[.]0[.]229[.]7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00741-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00741-01.pdf	

Imagen del sitio



CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00742-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
banchille-aumento-cupo[.]gq	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00742-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00742-01.pdf	

Imagen del sitio

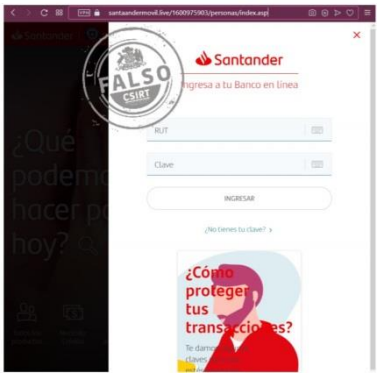


CSIRT informa de sitio que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00743-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
aumento-bancohile[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00743-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00743-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00744-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
banchille-aumento-cupos[.]ga	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00744-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00744-01.pdf	

Imagen del sitio

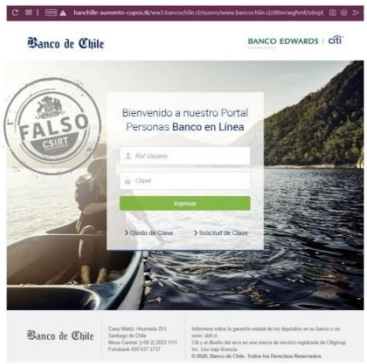


CSIRT advierte de web bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00745-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
santaandermovil[.]live	
IP	
162[.]213[.]255[.]51	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00745-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00745-01.pdf	

Imagen del sitio

CSIRT informa sobre portal que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00746-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
techwings[.]ae/actualizacion/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
166[.]62[.]28[.]79	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00746-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00746-01.pdf	

Imagen del sitio



CSIRT informa sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00747-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
banchille-aumento-cupos[.]tk	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00747-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00747-01.pdf	

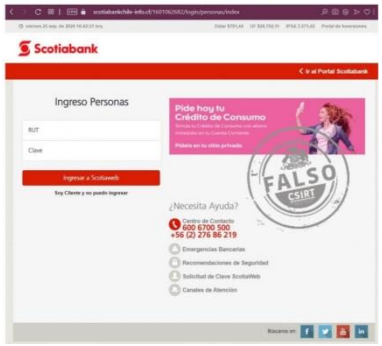
Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00748-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchile-infos[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00748-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00748-01.pdf	

Imagen del sitio

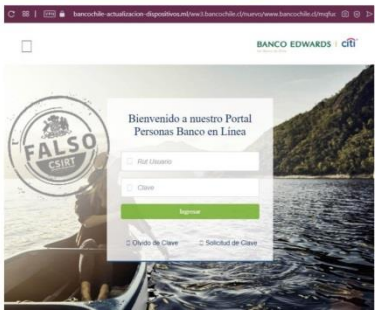
CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00749-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Septiembre de 2020
Última revisión	26 de Septiembre de 2020
Indicadores de compromiso	
URL	
segurisms-santan[.]website	
IP	
162[.]0[.]229[.]7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00749-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00749-01.pdf	

Imagen del sitio



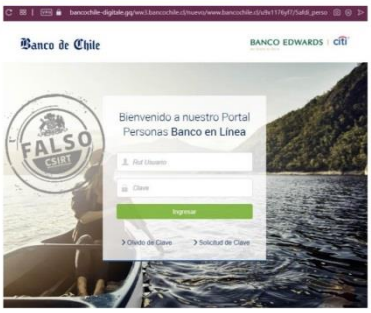
CSIRT informa sobre sitio que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00750-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Septiembre de 2020
Última revisión	26 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchile-info[.]cf	
IP	
91[.]234[.]99[.]119	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00750-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00750-01.pdf	

Imagen del sitio



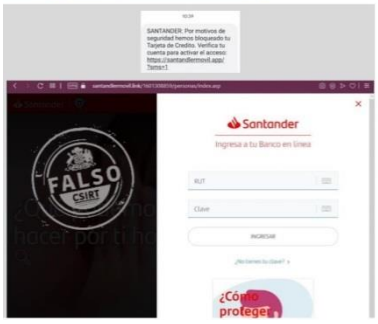
CSIRT advierte de portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00751-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Septiembre de 2020
Última revisión	26 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancochile-actualizacion-dispositivos[.]ml	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00751-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00751-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00752-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2020
Última revisión	25 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancochile-digitale[.]gq	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00752-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00753-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00753-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Septiembre de 2020
Última revisión	28 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://santandlermovil[.]app/?sms=1	
santandlermovil[.]link	
IP	
199[.]188[.]201[.]137	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00753-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00753-01.pdf	

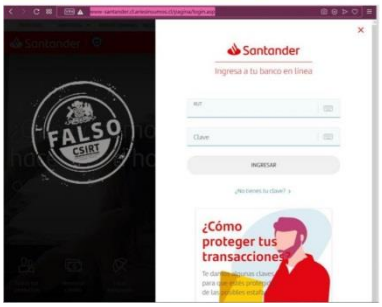
Imagen del sitio

CSIRT informa sobre sitio que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00754-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Septiembre de 2020
Última revisión	28 de Septiembre de 2020
Indicadores de compromiso	
URL	
scotiabankchle-infos[.]ml	
IP	
178[.]159[.]36[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00754-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00754-01.pdf	

Imagen del sitio

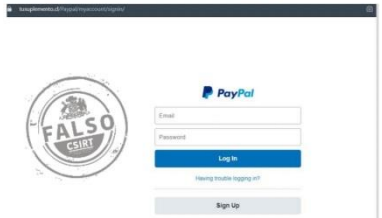
CSIRT advierte de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00755-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Septiembre de 2020
Última revisión	29 de Septiembre de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]ariesinsumos[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
199[.]58[.]186[.]108	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00755-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00755-01.pdf	

Imagen del sitio



CSIRT advierte de web de suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00756-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Septiembre de 2020
Última revisión	29 de Septiembre de 2020
Indicadores de compromiso	
URL	
www-santander[.]cl[.]ariesinsumos[.]cl/pagina/login[.]asp	
IP	
199[.]58[.]186[.]108	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00756-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00756-01.pdf	

Imagen del sitio



CSIRT advierte de portal que suplanta a sitio de pagos en línea	
Alerta de seguridad cibernética	8FFR20-00757-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Septiembre de 2020
Última revisión	29 de Septiembre de 2020
Indicadores de compromiso	
URL	
tusuplemento[.]cl/Paypal/myaccount/signin/	
IP	
198[.]57[.]244[.]93	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00757-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00757-01.pdf	

CSIRT advierte de sitio de streaming fraudulento	
Alerta de seguridad cibernética	8FFR20-00758-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
free-netflix[.]mr-19[.]com	
IP	
172[.]217[.]3[.]211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00758-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00758-01.pdf	

CSIRT advierte de portal de suplantación de sitio de streaming	
Alerta de seguridad cibernética	8FFR20-00759-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
netflixfreemium[.]xyz	
IP	
172[.]67[.]149[.]208	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00759-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00759-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta web de streaming	
Alerta de seguridad cibernética	8FFR20-00760-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
cpbild[.]co/d023d55	
IP	
99[.]86[.]38[.]67	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00760-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00760-01.pdf	

Imagen del sitio

CSIRT informa sobre portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00761-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
bancedelestado[.]ddns[.]net	
IP	
217[.]195[.]153[.]128	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00761-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00761-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00762-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]espaciocubico[.]cl	
IP	
162[.]241[.]48[.]174	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00762-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00762-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00763-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
bci-cl-demo[.]web[.]app/personas	
IP	
151[.]101[.]1[.]195	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00763-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00763-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio que suplanta portal bancario	
Alerta de seguridad cibernética	8FFR20-00764-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://sms1-santandr[.]website/?sms=1	
verifi-sms-santan[.]website	
IP	
151[.]101[.]1[.]195	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00764-01/	
https://www.csirt.gob.cl/media/2020/09/8FFR20-00764-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de smishing bancario por bloqueo de tarjeta	
Alerta de seguridad cibernética	8FPH20-00309-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2020
Última revisión	24 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://santaandermovil[.]live/1600976276/personas/index.asp	
IP	
162.213.255.51	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00309-01/	
https://www.csirt.gob.cl/media/2020/09/8FPH20-00309-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing bancario por operación irregular	
Alerta de seguridad cibernética	8FPH20-00310-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre de 2020
Indicadores de compromiso	
URL	
hxxps://santaandermovil[.]live/1600976276/personas/index.asp	
IP	
[146.185.218.43]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00310-01/	
https://www.csirt.gob.cl/media/2020/09/8FPH20-00310-01.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 (se recomienda bloquear)

0265e3d3a028211ab1cd17eb9336cdafce325e0f81859a201e792ef1b3fc2b34	7d78767f53a8a4b2cd5458d3fc8b2b9d66ffd2360e2b0ead6d83f5203fc3b5f2
02e90a20f8f565208e5d5723be87378e2c83733654b73e88667fcbed0c61ceab	7fe854ce78e7ab7cafcc299b4f2a4ee82cc366d47f9a8961727365e45688bb4c
0bcd0488b2252b2e84d4cea848215f0d67849215c10ab40efca305d9189e24c3	85c250bac6afbcff7c16c4cab2dd2653dc238fc483613bbf4c37b1fe3a6e8712
1665cb9b353605125840c136e4d1279f636adeb50027bcd91a86cb7bfea42e77	89955a5c1d24c93b26cad601eb0cabcc25ca816f51e264e4abbd1ec75de1b82f
185f4da81b1ccadae432ba82640736fc8e8e2bf32ac25f0283780ab885f10b26	8cfab9712cea12da9721200bd60d891ad5868d173a31260497d0dfac7919104d
1b0f925fe3ffc232052a970e10c587bac5a891476b2ed9d231a48a6db2c1b62a	9749f6f8e3963ea051833c57b14b70c86d6ce2df656353e790142a003bafd95c
3d9e5f07897b3089600b123a50a005eab5051640661dc4575c2afc0391c97ad8	a55dc088687d329d16c43578bd0bfe8b6716baada33a7488766252222336991 85
444a3aa13486d0771a92de61669b174ac0d22747d821cf2ff5fb334e1a574808	b8a9d5f54e75467b003cb37db317d9537fc49705aa3334531937929937b0eaae
479f549b2b68d98c8a2c7ead53fb42e5426084076981572c022aa746fb606b9c	baac09a30d626467916ed21abd6522e80bd2b584d89ebbfaf9cbbbd31e0fc49c
48523dc1483cef07ef0bca44fe8f6629de0a7ab7e89899640b66568d4816c54a	bd244207a04b13c2f19aa2ae6cfcb18baae07a101e2d455f3dc45224e7540b80
4c321ed11d6a36c829d1a7e5f32dd1370d9535d40779665a2dbb32a74653c25d	cd9fc40801696d68bd1926c4f276fedb3a3e857dcfc5c758c43de0e5d2c86173
51f9944b31644a2669f782903d89af7917d19955ef108fe80b43ea64466d7259	cdbdac72c0c2faaa469f1e1f0ca1c6f026d3cf1246c1ac99ee261846f67bea4b
600c433856179a39c24e978c417634772d605b733afea857de865c8ff787105f	d15f6feb5c2c80a5218fbac4d8293c0eef906fbc9b6522f690b63f1411bd6ee9
6437fef16a0ec7636fd1b9e2179d73261cfd2c9a995063ced4498e3400f1e3b4	da86de2e8d0fcec9820a7cfe23a969be0aa5b7d4e281fa92481c33346a57df0b
66a11e15a35b99f47141c96eea0b9ed06dabec96652bd31e5624f3c1e0146f2e	e39f691edc4ff1e1fe413e85f4ac03ceace139451e760efb67e195bdd940da7f
fd9bb0c16419fd87e7d7dcb84e3969d4480b8dfd441706cf8a2050770a84b76a	ed86c762a5e44ef00d204c142dc87289cc87ae629caf7fcf46b1e950f3198ee2

Archivos reportados (se recomienda mantener en monitoreo)

61.219.196.150	201.76.49.200
86.109.161.190	201.76.49.203
116.202.197.180	201.76.49.232
136.243.193.153	201.76.49.233
190.128.238.206	201.76.49.234
209.114.133.142	201.76.49.235
213.192.239.117	201.76.49.50
213.227.155.247	201.76.49.52
118.69.190.130	201.76.49.53
157.230.90.221	201.76.49.54
157.230.94.251	201.76.49.56
157.7.245.221	201.76.49.57
162.241.91.62	201.76.49.58

165.227.130.72	216.70.115.251
172.93.201.196	45.137.22.75
176.74.29.118	45.137.22.84
181.40.114.234	68.183.76.224
191.252.14.6	82.223.98.30
200.11.30.190	89.46.69.36
95.216.23.195	

Correo electrónico (Se recomienda mantener monitoreo)

aatri7@gmail.com	isabellgreg171rj@gmail.com
ady.bravo@pddh.gob.ni	isendana0iwony@gmail.com
ahsan@afccl.asia	jacqalon41rucir@gmail.com
aldo.godoy@cavallaro.com.py	javier.cavallaro@mobilepy.com
alexflores@thorsman.com.mx	ketcdutj170tyue@gmail.com
allprint@terra.cl	kimgarr459ohno@gmail.com
amadeoficina@terra.cl	koepketemi17uorao@gmail.com
anna@vogiacorp.vn	lambertkeng249oe@gmail.com
appadurai.designistic@gmail.com	mayara@hortsoy.com.br
audrey@915.gonbino.ml	mdl@updi.net
bosun@hinckley.com.ng	milton.r.blount@newmountolivet.org
burkelynn19z@gmail.com	noelia@insmagas.com
buviregi380tatuu@gmail.com	ordini@woodstyleinfissi.it
cus9@jhship.com.cn	robert@luxware.net
dysonkizz7mvuj@gmail.com	rodolfo@edilmag.it
elifakturk@cofcointernational.com	sales@sovio.com
engvinicius@tanktest.com.br	shipping@hysong.cn
expedicao02@g5interlog.com.br	solizbula031co@gmail.com
fax@maspi.es	sr@psdelta.com
furuhashi@mskinc.co.jp	stepnoah502jytuw@gmail.com
glenshan72zurie@gmail.com	tacila@turismo10alphaville.tur.br
harremme142kfmei@gmail.com	trojlita384hrk@gmail.com
hse@binjarra.com	varga@grandbari.sk
info@starfoxsecu.com	vendas@genova.ind.br
info@transfopam.com	Wendy.Fu@sbdinc.com
info@uvmkt.com	whitejoye45qenau@gmail.com

URL

hxxp://hbprivileged[.]com/info/S/
hxxp://equipamentosmix[.]com/10/U/
hxxp://mianusman[.]com/cgi-bin/Fo/
hxxps://www[.]hairlineunisexsalon[.]com/demo/CyD/
hxxp://liulibug[.]com/wp-admin/8Aw/
hxxps://fcbc[.]group/wp-includes/O/
hxxp://khobormalda[.]com/wp-content/82/
hxxp://blog[.]zunapro[.]com/wp-admin/LEE/
hxxp://megasolucoesti[.]com/R9KDq0O8w/Y/

hxxps://online24h[.]biz/wp-admin/K/
hxxps://fepami[.]com/wp-includes/eal/
hxxp://ora-ks[.]com/system/cache/w/
hxxp://padamagro[.]com/wp-admin/Nc/
hxxp://h2a1[.]com/uf8vu/U/
hxxp://www[.]almakaaseb[.]com/wp-includes/P/
hxxp://theitnconsultant[.]com/wp-includes/t/
hxxp://carstarai[.]com/icon/D/
hxxp://bug[.]chihuahuamediaprojects[.]com/wp-includes/u/
hxxps://aecc[.]dev[.]caveim[.]net/wp-admin/dZ/
hxxp://phimsex[.]2xxhub[.]com/wp-content/esp/5ur8drbma/6qH/

Actualidad

Revista Cibersucesos n°3

El Equipo de Respuesta Ante Incidentes de Seguridad Informática, CSIRT, publicó la tercera edición de "Cibersucesos", dedicada al emprendimiento, al desarrollo de la industria, los desarrollos propios del CSIRT y la protección de la propiedad intelectual.

Ver más: https://www.csirt.gob.cl/recomendaciones/revista-cibersucesos-n3/

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 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.

- Marco Almonacid
- Álvaro Pacheco
- Nancy Zapata

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.10.02 17:02:25 -03'00'