30-07-2020 | Año 2 | N°56

Boletín de Seguridad Cibernética

Semana del 23 al 29 de julio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

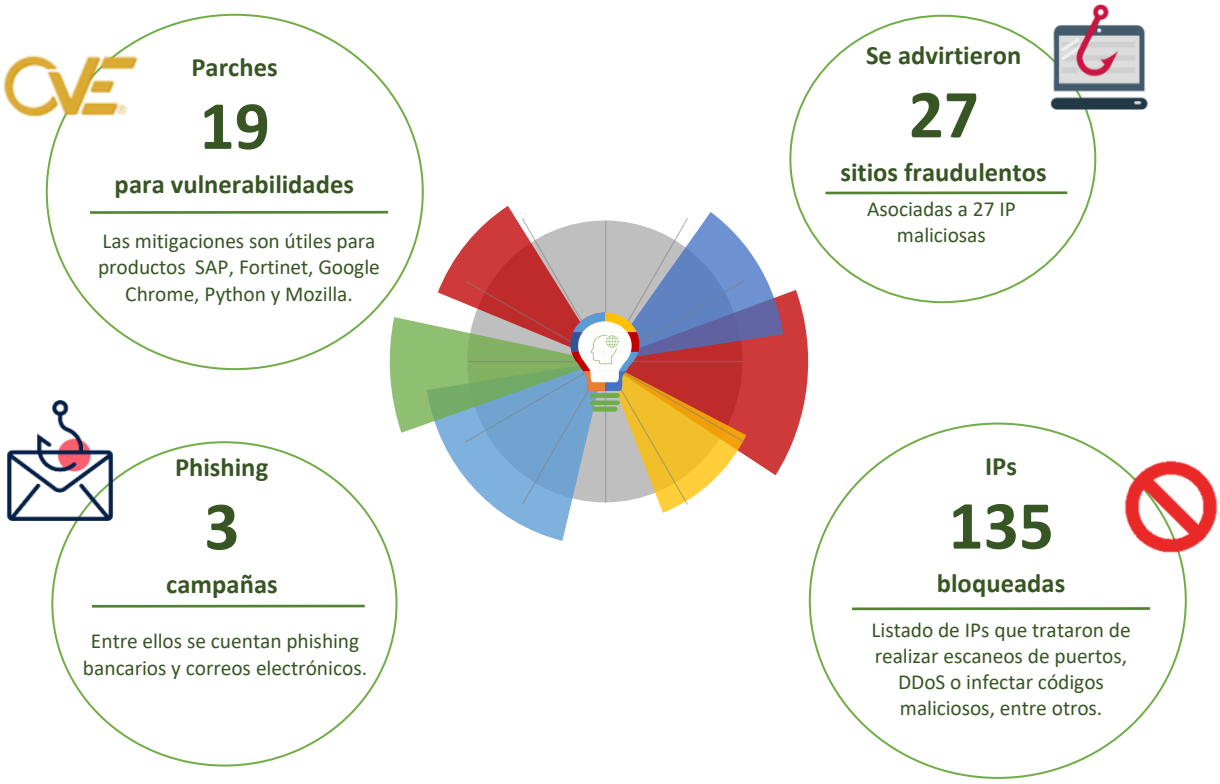
División de Redes y Seguridad Informática.

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

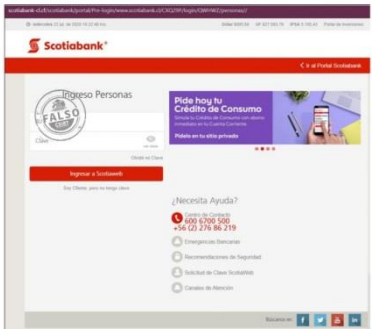
Sitios fraudulentos 3
Phishing 17
Vulnerabilidades 19
Indicadores de Compromisos 22
Recomendaciones y Buenas Prácticas 22
Investigación 25
Muro de la Fama 27

Sitios fraudulentos

Imagen del sitio

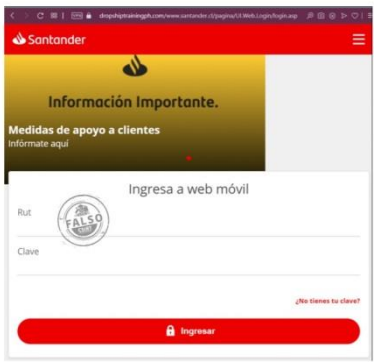
CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00534-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
Indicadores de compromiso	
URL	
flycca[.]cz/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]27[.]143[.]60v	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00534-01-2/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00534-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00535-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
Indicadores de compromiso	
URL	
scotiabank-cl[.]cf	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00535-01-2/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00535-01.pdf	

Imagen del sitio

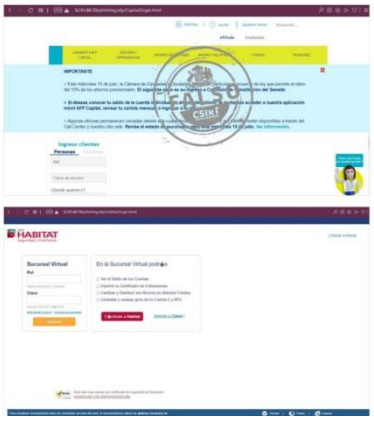


CSIRT informa sobre sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00536-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
Indicadores de compromiso	
URL	
dropshiptrainingph[.]com/www[.]santander[.]cl/pagina/UI[.]Web[.]Login/login[.]asp	
IP	
185[.]150[.]191[.]224	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0536-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00536-01.pdf	

Imagen del sitio

CSIRT advierte de sitio banacario fraudulento	
Alerta de seguridad cibernética	8FFR20-00537-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
Indicadores de compromiso	
URL	
allshop[.]cz/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]27[.]171[.]200	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00537-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00537-01.pdf	

Imagen del sitio



CSIRT advierte de sitio fraudulento de AFP	
Alerta de seguridad cibernética	8FFR20-00538-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
Indicadores de compromiso	
URL	
52[.]91[.]80[.]70/phishing/afp/Capital/login[.]html	
52[.]91[.]80[.]70/phishing/afp/Habitat/login[.]html	
52[.]91[.]80[.]70/phishing/afp/Modelo/login[.]html	
52[.]91[.]80[.]70/phishing/afp/Planvital/login[.]html	
52[.]91[.]80[.]70/phishing/afp/Provida/login[.]html	
IP	
52[.]91[.]80[.]70	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00538-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00538-01.pdf	

Imagen del sitio

CSRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00539-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]login-bchile[.]ml/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl/63TPVX/login/NCDSC/personas//	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00539-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00539-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta a banco	
Alerta de seguridad cibernética	8FFR20-00540-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
bodex[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]27[.]150[.]136	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00540-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00540-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00541-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
portal-bancestado[.]ga/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00541-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00541-01.pdf	

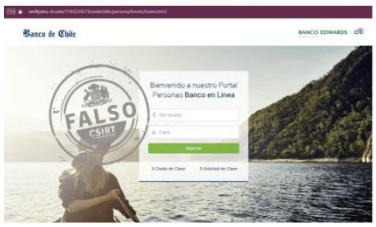
Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00542-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]login-bchile[.]cf	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00542-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00542-01.pdf	

Imagen del sitio

CSIRT informa de portal de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00543-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado-personas[.]website/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]187[.]29[.]20	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00543-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00543-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00544-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
verifysms-cl[.]com/1595528578/webchile/persona/home/index[.]html	
IP	
162[.]0[.]232[.]56	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00544-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00544-01.pdf	

Imagen del sitio

CSIRT informa de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00545-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
gamtur[.]lv/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]27[.]148[.]227	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00545-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00545-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00546-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
danilov[.]lv/www[.]santander[.]cl/pagina/login[.]asp	
IP	
172[.]67[.]173[.]26	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00546-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00546-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta a web bancaria	
Alerta de seguridad cibernética	8FFR20-00547-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]filestube[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]18[.]41[.]11	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0547-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00547-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00548-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado-app[.]website	
IP	
68[.]65[.]123[.]130	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00548-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00548-01.pdf	

Imagen del sitio

CSIRT informa de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00549-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
bancochile[.]cl[.]mget[.]com[.]br	
IP	
54[.]39[.]28[.]233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00549-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00549-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00550-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
acceso[.]banconchile[.]live	
IP	
109[.]234[.]35[.]78	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0550-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00550-01.pdfyg5tf	

Imagen del sitio

CSIRT informa de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00551-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancochile[.]cl[.]studioretrofit[.]com[.]br	
IP	
54[.]39[.]28[.]233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00551-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-0551-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00552-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
bancoesto-bchile[.]ga/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0552-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00552-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00553-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2020
Última revisión	25 de Julio de 2020
Indicadores de compromiso	
URL	
home-smsverifycl[.]com/1595618836/webchile/persona/home/index[.]html	
IP	
162[.]0[.]232[.]55	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0553-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00553-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00554-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestdo-home[.]cf/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0554-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00554-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00555-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
Indicadores de compromiso	
URL	
tarjetacencosud-cl-home[.]ga/tarjetacencosud/nuevo/www[.]tarjetacencosud[.]cl/Tarjeta/	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00555-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00555-01.pdf	

Imagen del sitio

CSIRT informa de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00556-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado[.]com[.]de/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
104[.]219[.]248[.]95	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0556-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00556-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00557-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]leedshr[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
103[.]14[.]121[.]172	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0557-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00557-01.pdf	

Imagen del sitio

CSIRT informa de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00558-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
Indicadores de compromiso	
URL	
homebchile[.]movil-online[.]com/1595873401/webchile/persona/home/index[.]html	
IP	
185[.]69[.]53[.]41	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00558-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00558-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00559-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestdo[.]ga/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00559-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00559-01.pdf	

Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00560-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2020
Última revisión	29 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestdo[.]ga/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
104[.]219[.]248[.]102	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0560-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00560-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de phishing bancario por crédito FOGAPE	
Alerta de seguridad cibernética	8FPH20-00273-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps[:]//idln.kemdikbud.go[.]id/w.php	
https[:]//bancoesto-bchile[.]tk//imagenes/comun2008/banca-en-linea-personas.html	
https[:]//bancoesto-bchile[.]gq//imagenes/comun2008/banca-en-linea-personas.html	
IP	
[103.248.146.11]	
[170.10.161.204]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00273-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00273-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing bancario por crédito FOGAPE	
Alerta de seguridad cibernética	8FPH20-00274-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Julio de 2020
Última revisión	27 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://www.azadiclub[.]ir/cli/enviar02.php?l=1420247376	
hxxp://nezhalska[.]com/activacion/cuenta-loqt/	
hxxps://www.leedshr[.]com/www.santander.cl/pagina/login.asp	
IP	
[170.239.87.149]	
[104.218.63.83]	
[103.52.44.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00274-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00274-01.pdf	

CSIRT advierte de phishing de servicio de streaming	
Alerta de seguridad cibernética	8FPH20-00275-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Julio de 2020
Última revisión	27 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://inicia.nefllxapp.leksz[.]com/login_cl_4enp/premium/actualiza.php	
IP	
[195.88.158.6]	
[67.225.172.19]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00275-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00275-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidad y mitigación obtenida de Cisco	
Alerta de seguridad cibernética	9VSA20-00277-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Julio de 2020
Última revisión	23 de Julio de 2020
CVE	
Cve-2020-3452	
Fabricante	
Cisco	
Productos afectados	
Esta vulnerabilidad afecta a los productos de Cisco si están ejecutando una versión vulnerable de Cisco ASA Software o Cisco FTD Software con una configuración vulnerable de AnyConnect o WebVPN.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00277-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA-00277-01.pdf	

CSIRT comparte actualizaciones de Joomla!	
Alerta de seguridad cibernética	9VSA20-00278-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2020
Última revisión	24 de Julio de 2020
CVE	
CVE-2020-15699 - CVE-2020-15695 - CVE-2020-15697 CVE-2020-15696 - CVE-2020-15698 - CWE-352 – [20200701]	
Fabricante	
Fortinet	
Productos afectados	
Gestor de contenidos Joomla! desde la versión 2.5.0 hasta la 3.9.19. Gestor de contenidos Joomla! desde la versión 3.9.0 hasta la 3.9.19.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00278-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00278-01.pdf	

CSIRT comparte información obtenida de ClamAV	
Alerta de seguridad cibernética	9VSA20-00279-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2020
Última revisión	28 de Julio de 2020
CVE	
CVE-2020-3350 - CVE-2020-3327 - CVE-2020-3481	
Fabricante	
ClamAV	
Producto afectado	
ClamAV versiones anteriores a la 0.102.4. ClamAV versión 0.102.3. ClamAV entre la versión 0.102.0 y la 0.102.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00279-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00279-01.pdf	

CSIRT comparte actualizaciones obtenidas de Moodle	
Alerta de seguridad cibernética	9VSA20-00280-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2020
Última revisión	29 de Julio de 2020
CVE	
CVE-2020-14320 - CVE-2020-14321 - CVE-2020-14322	
Fabricante	
Moodle	
Productos afectados	
Moodle versiones 3.9, 3.8 – 3.8.3 y 3.7 – 3.7.6. Moodle versiones 3.9, 3.8 – 3.8.3, 3.7 – 3.7.6, 3.5 – 3.5.12 y versiones anteriores no soportadas.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00280-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00280-01.pdf	

CSIRT advierte vulnerabilidades y comparte mitigaciones obtenidas de Google Chrome	
Alerta de seguridad cibernética	9VSA20-00275-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2020
Última revisión	29 de Julio de 2020
CVE	
CVE-2020-6537 - CVE-2020-6538 - CVE-2020-6532 CVE-2020-6539 - CVE-2020-6540 - CVE-2020-6541	
Fabricante	
Google Chrome	
Producto afectado	
Versiones anteriores a la 84.0.4147.105.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00281-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00281-01.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:

IP	Motivo	IP	Motivo
185.156.175.59	DDoS	74.206.99.220	Port Scan
199.249.230.17	DDoS	5.182.211.17	Port Scan
199.249.230.7	DDoS	162.241.73.2	Port Scan
184.75.223.235	DDoS	80.82.65.105	Port Scan
64.42.179.67	DDoS	161.97.87.68	Port Scan
68.235.35.124	DDoS	159.65.10.4	Port Scan
184.75.221.195	DDoS	194.32.78.159	Port Scan
199.249.230.22	DDoS	50.234.173.102	Port Scan
80.211.32.88	Malware	177.220.191.137	Port Scan
211.20.154.102	Malware	65.124.71.68	Port Scan
187.207.207.16	Malware	59.188.236.36	Port Scan
103.237.79.187	Malware	64.56.66.180	Port Scan
45.118.136.92	Malware	205.205.150.20	Port Scan
163.172.107.70	Malware	185.217.1.244	Port Scan
190.164.75.175	Malware	89.248.168.17	Port Scan
212.156.133.218	Malware	45.148.121.143	Port Scan
78.188.170.128	Malware	212.129.40.33	Port Scan
113.161.148.81	Malware	133.242.49.56	Port Scan
177.0.241.28	Malware	192.241.234.95	Port Scan
157.245.47.152	Port Scan	103.145.12.10	Port Scan
185.156.175.59	Port Scan	2.57.122.196	Port Scan
188.148.158.192	Port Scan	185.234.218.36	Port Scan
45.129.33.4	Port Scan	104.248.173.78	Port Scan
156.96.117.172	Port Scan	138.246.253.5	Port Scan
161.97.64.44	Port Scan	45.145.66.120	Port Scan
45.148.121.134	Port Scan	45.129.33.18	Port Scan
192.241.234.107	Port Scan	45.129.33.20	Port Scan
192.241.234.29	Port Scan	45.129.33.17	Port Scan
113.172.29.65	Port Scan	45.129.33.22	Port Scan
192.241.222.11	Port Scan	45.129.33.19	Port Scan

192.241.211.223	Port Scan	94.102.49.191	Port Scan
51.210.113.108	Port Scan	80.82.78.82	Port Scan
192.241.214.159	Port Scan	185.132.249.244	Port Scan
5.182.210.205	Port Scan	192.241.234.8	Port Scan
199.115.114.9	Port Scan	185.132.249.201	Port Scan
202.101.173.130	Port Scan	94.102.51.77	Port Scan
104.244.76.86	Port Scan	185.200.118.71	Port Scan
192.87.30.70	Port Scan	103.133.110.166	Port Scan
209.141.47.222	Port Scan	45.129.33.6	Port Scan
199.249.230.37	Port Scan	64.56.66.180	Port Scan
37.49.230.49	Port Scan	45.129.33.10	Port Scan
156.96.117.57	Port Scan	161.35.218.147	Port Scan
192.241.230.237	Port Scan	103.145.12.204	Port Scan
192.241.210.45	Port Scan	128.14.141.100	Port Scan
188.165.126.60	Port Scan	129.227.129.164	Port Scan
185.200.118.48	Port Scan	125.227.196.145	Port Scan
217.182.36.107	Port Scan	180.242.181.179	Port Scan
192.241.212.45	Port Scan	103.145.12.14	Port Scan
185.228.19.147	Port Scan	192.99.32.54	Port Scan
194.36.111.59	Port Scan	185.200.118.50	Port Scan
91.132.0.203	Port Scan	45.143.223.88	Port Scan
103.145.12.206	Port Scan	128.14.141.101	Port Scan
192.99.98.81	Port Scan	89.248.174.166	Port Scan
49.204.143.215	Port Scan	190.237.30.119	Spam
192.241.222.214	Port Scan	77.243.27.240	Spam
51.222.33.62	Port Scan	109.64.22.107	Spam
45.143.220.37	Port Scan	103.57.121.22	XSS
148.72.158.112	Port Scan	117.58.245.114	XSS
108.62.103.212	Port Scan	117.58.245.114	XSS
161.35.218.147	Port Scan	167.250.6.40	XSS
167.71.14.75	Port Scan		

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.

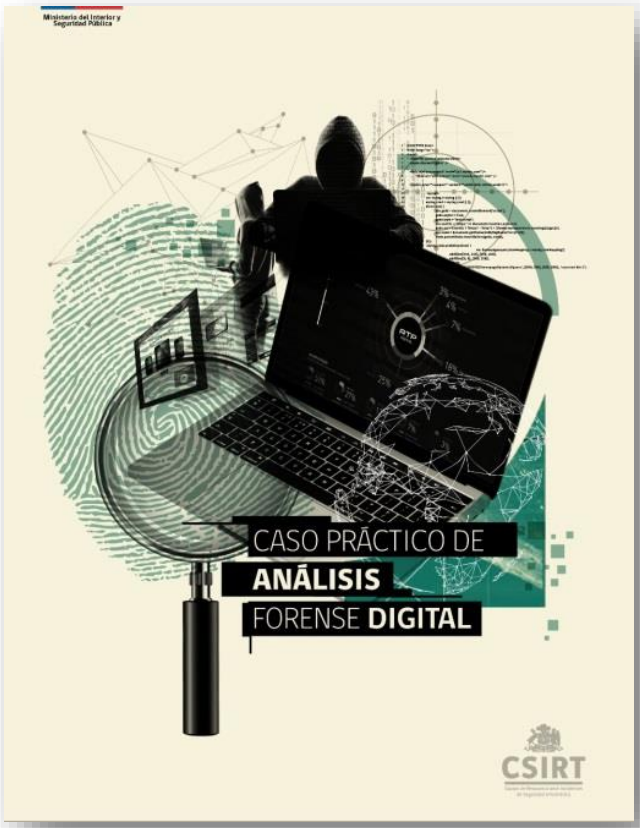
Investigación

Caso Práctico de Análisis Forense Digital

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la décimo segunda edición de su publicación sobre amenazas cibernéticas el que analiza un caso práctico de análisis forense. Este artículo fue elaborado por Andrés Godoy Pérez, analista forense independiente y colaborador de CSIRT.

El Análisis Forense Digital (AFD) se define como el proceso que aborda diversas etapas en el tratamiento de evidencia digital, entre ellas están las de identificación, preservación, recolección, transporte, análisis y presentación de resultados acorde a los procesos legalmente aceptados y sus correspondientes procedimientos formales en cada país.

En este artículo veremos en profundidad cómo fijar la evidencia, montar evidencia digital en SIFT Workstation, buscar indicadores de compromiso y dejaremos enunciados los pasos siguientes del análisis: Gestión de Indicadores de Compromiso e Informe forense.



Ver más en: https://www.csirt.gob.cl/reportes/an2-2020-12/

Actualidad

Ciberconsejos para evitar estafas en la operación devolución de tu 10% de AFP

La aprobación del retiro del 10% de los fondos de las AFP, han incentivado a los ciberdelincuentes para crear estrategias que buscan engañar a las personas con el objetivo de apropiarse de sus recursos utilizando nuevas campañas de phishing. Si estás pensando en solicitar tu 10%, toma precauciones y cuídate para no perder tu devolución de 10% de AFP.

Ver en: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-estafas-en-la-operacion-devolucion-de-tu-10-de-afp/

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.

- Joseph De Freitas
  Linkedin:
  https://www.linkedin.com/in/joseph-de-freitas-7480b964/
- Daniel Torres
- Alexander Vianney
- Óscar Guarda
  Linkedin:
  https://www.linkedin.com/in/oscar-guarda/
- Cristian Salinas
- Andrés Vera
  Linkedin:
  https://www.linkedin.com/in/andres-eduardo-vera-acu%C3%B1a-31623a2b/
- Darsy Lescano

CSIRT Gobierno de Chile Firmado digitalmente por CSIRT Gobierno de Chile Fecha: 2020.07.31 18:21:02 -04'00'