16-07-2020 | Año 2 | N°54

Boletín de Seguridad Cibernética

Semana del 09 al 15 de julio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

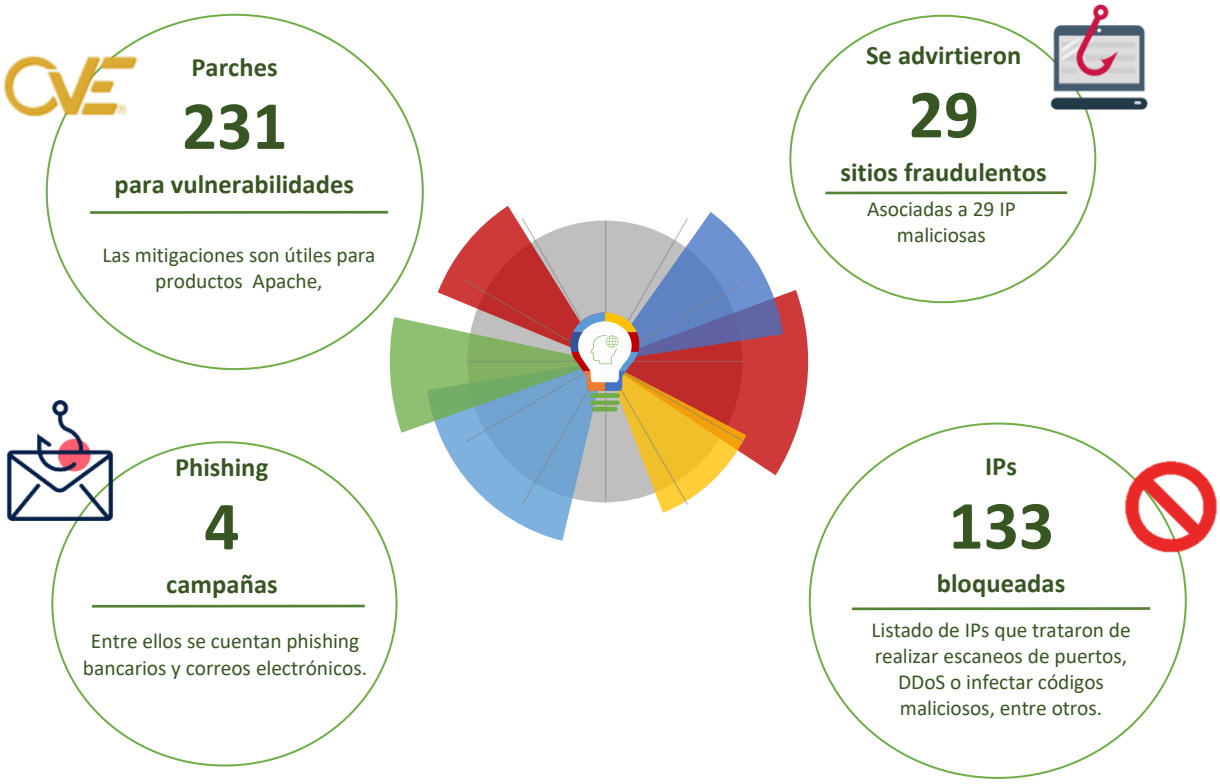
División de Redes y Seguridad Informática.

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

Imagen del sitio

CSIRT informa de portal bancario utilizado para fraudes	
Alerta de seguridad cibernética	8FFR20-00479-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
Indicadores de compromiso	
URL	
estado[.]chilesecuritymobile[.]com/site/index[.]php	
IP	
195[.]189[.]96[.]36	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00479-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00479-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00480-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado[.]cl[.]wandja-djoumessi[.]com/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
162[.]144[.]255[.]96	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00480-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00480-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00481-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestaido[.]com/1594244296/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
185[.]61[.]154[.]31	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00481-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00481-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00482-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado-sms[.]000a[.]biz/bancoestado/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
185[.]27[.]134[.]100	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00482-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00482-01.pdf	

Imagen del sitio

CSIRT informa sobre web utilizada para fraudes bancarios	
Alerta de seguridad cibernética	8FFR20-00483-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
Indicadores de compromiso	
URL	
acceso.banconchile[.]net/mypes-an95ZqWYoJJqq5JnpLKX	
IP	
86[.]106[.]20[.]170	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00483-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00483-01.pdf	

Imagen del sitio

CSIRT advierte sobre sitio fraudulento bancario	
Alerta de seguridad cibernética	8FFR20-00484-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
Indicadores de compromiso	
URL	
wamatechnology[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
216[.]10[.]240[.]90	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00484-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00484-01.pdf	

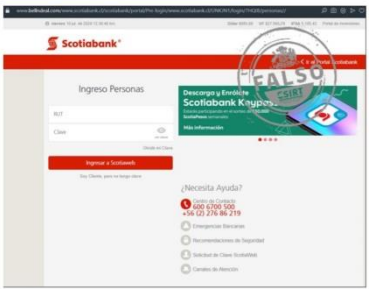
Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00485-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
Indicadores de compromiso	
URL	
banco[.]acessoestado[.]com	
IP	
195[.]189[.]96[.]36	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0085-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00485-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00486-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]scotiabanckcl[.]com	
IP	
107[.]175[.]33[.]24	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0086-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00486-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00487-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Julio de 2020
Última revisión	11 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]bellndeal[.]com/www[.]scotiabank[.]cl/scotiabank/portal/Pre-login/	
IP	
46[.]4[.]227[.]96	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0087-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00487-01.pdf	

Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00488-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Julio de 2020
Última revisión	11 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]sahifa-news[.]com/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
23[.]235[.]221[.]30	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00488-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00488-01.pdf	

Imagen del sitio

CSIRT informa de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00489-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Julio de 2020
Última revisión	11 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancestado[.]gotdns[.]ch	
IP	
208[.]123[.]119[.]102	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00489-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00489-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00490-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Julio de 2020
Última revisión	11 de Julio de 2020
Indicadores de compromiso	
URL	
142[.]11[.]239[.]103/bancoestado-bancapersonas/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
142[.]11[.]239[.]103	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00490-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00490-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00491-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]www-bancoestado[.]cl[.]dev[.]decorativescreensdirect[.]com[.]au/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
103[.]28[.]49[.]63	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00491-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00491-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00492-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancoestado[.]cl[.]erikteichmann[.]com/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
158[.]69[.]11[.]191	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00492-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00492-01.pdf	

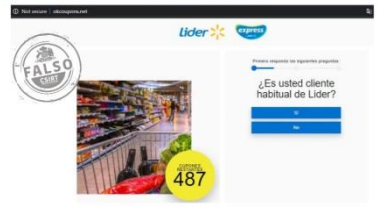
Imagen del sitio

CSIRT advierte de sitio de tarjeta de crédito fraudulento	
Alerta de seguridad cibernética	8FFR20-00493-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]htlp-wwv-crnr-cl[.]mitsp[.]org/personas-cl/	
IP	
162[.]144[.]123[.]218	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00493-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00493-01.pdf	

Imagen del sitio

CSIRT advierte sobre portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00494-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]banvcoestado[.]com	
IP	
54[.]36[.]145[.]173	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00494-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00494-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de supermercado fraudulento	
Alerta de seguridad cibernética	8FFR20-00495-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
okcoupons[.]net	
IP	
45[.]148[.]120[.]2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00495-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00495-01.pdf	

Imagen del sitio

CSIRT advierte de sitio fraudulento sobre covid-19	
Alerta de seguridad cibernética	8FFR20-00496-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
alfkar[.]com/registrate/?mx#	
IP	
160[.]153[.]133[.]151	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00496-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00496-01.pdf	

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00497-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
mercadom[.]com[.]ar/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
162[.]0[.]229[.]11	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00497-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00497-01.pdf	

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00498-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancoestado-cl[.]hothfactory[.]com/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
173[.]249[.]54[.]180	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00498-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00498-01.pdf	

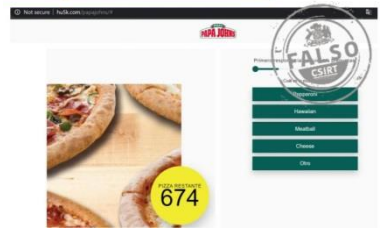
Imagen del sitio

CSIRT advierte de sitio fraudulento sobre covid-19	
Alerta de seguridad cibernética	8FFR20-00499-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]quedateencas[.]com/#	
IP	
216[.]239[.]36[.]21	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00499-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00499-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de streaming fraudulento	
Alerta de seguridad cibernética	8FFR20-00500-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
hu5k[.]com/Netflix	
IP	
160[.]153[.]133[.]157	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00500-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00500-01.pdf	

Imagen del sitio



CSIRT advierte de sitio que suplanta a web de cadena de pizzería	
Alerta de seguridad cibernética	8FFR20-00501-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
hu5k[.]com/papajohns/#	
IP	
160[.]153[.]133[.]157	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00501-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00501-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario suplantado para cometer fraudes	
Alerta de seguridad cibernética	8FFR20-00502-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
acceso[.]bancochlie[.]website	
IP	
38[.]132[.]99[.]223	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00502-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00502-01.pdf	

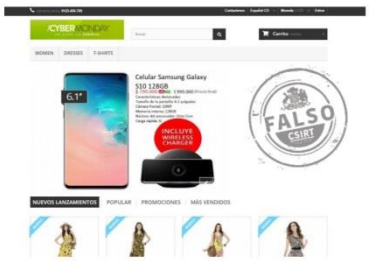
Imagen del sitio

CSIRT advierte de sitio que suplanta web de cadena de hamburguesas	
Alerta de seguridad cibernética	8FFR20-00503-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
hu5k[.]com/burger/#	
IP	
160[.]153[.]133[.]157	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00503-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00503-01.pdf	

Imagen del sitio

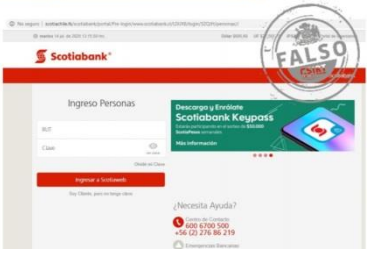
CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00504-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
bancapersonas-bancoestado[.]cl[.]onetoone[.]cl/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
200[.]73[.]115[.]38	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00504-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00504-01.pdf	

Imagen del sitio



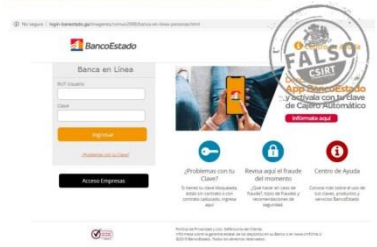
CSIRT advierte de sitio que suplanta a tienda por departamentos	
Alerta de seguridad cibernética	8FFR20-00505-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
falabella[.]cyberday-smartphone[.]com/index[.]php	
IP	
190[.]107[.]177[.]58	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00505-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00505-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00506-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
scotiachile[.]tk/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl/LDIJX8/login/3ZQJH/personas//	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00506-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00506-01.pdf	

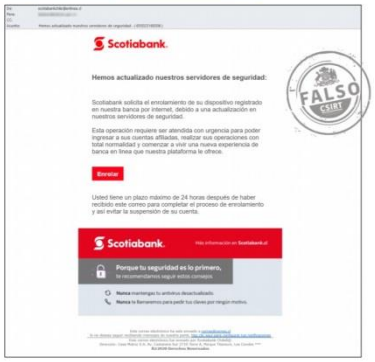
Imagen del sitio



CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00507-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
URL	
login-banestado[.]ga/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00507-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00507-01.pdf	

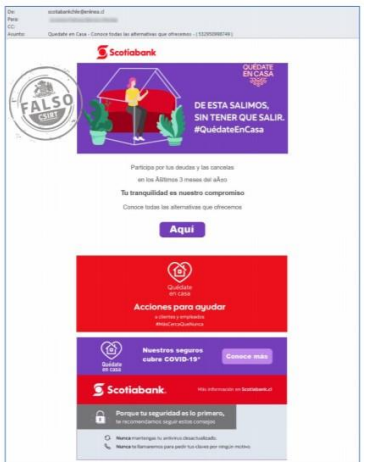
Phishing

Imagen del mensaje



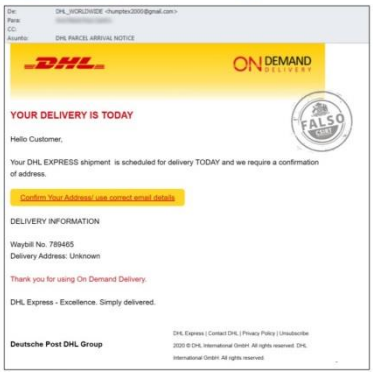
CSIRT advierte de phishing bancario por actualización de dispositivo	
Alerta de seguridad cibernética	8FPH20-00265-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://elec-brico[.]fr/home[.]php	
hxxps://www.bellndeal.com/www.scotiabank.cl/nuevo/scotiabank/portal/Pre-login/www.scotiabank.cl/RK8WX2/login/YOANU/personas//	
IP	
[103.248.146.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00265-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00265-01.pdf	

Imagen del mensaje



CSIRT advierte de phishing bancario por promoción	
Alerta de seguridad cibernética	8FPH20-00266-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Julio de 2020
Última revisión	13 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://vitrinesdemetz[.]com/key[.]php	
hxxp://elec-brico[.]fr/click[.]php	
hxxps://scotiachile[.]ga/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl	
IP	
[103.248.146.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00266-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00266-01.pdf	

Imagen del mensaje



CSIRT advierte de phishing por falso envío de encomienda	
Alerta de seguridad cibernética	8FPH20-00267-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://storage[.]googleapisvcom/dhl-parcel-tracking[.]appspot[.]com/trackingdeliveryorderesupdateshere/DHL[.]html	
IP	
[124.110.96.72]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00267-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00267-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por millonaria compensación	
Alerta de seguridad cibernética	8FPH20-00268-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Julio de 2020
Última revisión	15 de Julio de 2020
Indicadores de compromiso	
IP	
[77.92.152.35]	
[77.92.152.37]	
[77.92.152.38]	
[78.135.113.146]	
[188.132.180.38]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00268-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00268-01.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones para productos Huawei	
Alerta de seguridad cibernética	9VSA20-00264-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
CVE	
CVE-2020-1838 - CVE-2020-9263 - CVE-2020-9262 CVE-2020-9261 - CVE-2020-1839 - CVE-2020-12695 CVE-2020-9100	
Fabricante	
Huawei	
Productos afectados	
Huawei Mate 30 Pro versiones anteriores a la 10.1.0.150(C00E136R5P3). Huawei Mate 30 versiones anteriores a la 10.1.0.150(C00E136R5P3). Huawei Mate 30 versiones anteriores a la 10.0.5.1(H612SP5C233).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00264-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00264-01.pdf	

CSIRT comparte actualizaciones obtenidas de Mozilla	
Alerta de seguridad cibernética	9VSA20-00265-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
CVE	
CVE-2020-12415, CVE-2020-12416, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12402, CVE-2020-12421, CVE-2020-12422, CVE-2020-12423, CVE-2020-12424, CVE-2020-12425, CVE-2020-12426, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, CVE-2020-12421, CVE-2020-12417, CVE-2020-12418, CVE-2020-12419, CVE-2020-12420, MFSA-2020-0001, CVE-2020-12421, MFSA-2020-0002	
Fabricante	
Mozilla	
Productos afectados	
Firefox versiones anteriores a la 78., Firefox ESR versiones anteriores a la 68.10., Thunderbird versiones anteriores a la 68.10., Firefox para Android.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00265-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00265-01.pdf	

CSIRT comparte vulnerabilidad y mitigación para PHP Mailer	
Alerta de seguridad cibernética	9VSA20-00266-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
CVE	
CVE-2020-13625	
Fabricante	
PHP Mailer	
Producto afectado	
PHPMailer versión 6.1.5 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00266-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00266-01.pdf	

CSIRT comparte vulnerabilidad y mitigación obtenida de Apache Spark	
Alerta de seguridad cibernética	9VSA20-00267-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Julio de 2020
Última revisión	09 de Julio de 2020
CVE	
CVE-2020-9480	
Fabricante	
Apache	
Productos afectados	
Apache Spark versión 2.4.5 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00267-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00267-01.pdf	

CSIRT comparte actualizaciones de Juniper	
Alerta de seguridad cibernética	9VSA20-00268-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020

CVE

CVE-2020-4274 - CVE-2017-3164 - CVE-2020-4294
CVE-2019-2989 - CVE-2019-2975 - CVE-2019-2981
CVE-2019-2973 - CVE-2019-2964 - CVE-2019-4593
CVE-2020-4272 - CVE-2020-4270 - CVE-2020-4269
CVE-2019-4594 - CVE-2020-4268 - CVE-2020-4271
CVE-2019-4654 - CVE-2018-0734 - CVE-2019-4508
CVE-2019-17359 - CVE-2018-1000613 - CVE-2018-1000180
CVE-2018-5382 - CVE-2017-13098 - CVE-2016-1000352
CVE-2016-1000346 - CVE-2016-1000345 - CVE-2016-1000344
CVE-2016-1000343 - CVE-2016-1000342 - CVE-2016-1000341
CVE-2016-1000340 - CVE-2016-1000339 - CVE-2016-1000338
CVE-2016-2427 - CVE-2015-7940 - CVE-2013-1624
CVE-2007-6721 - CVE-2020-1650 - CVE-2020-1651
CVE-2020-1649 - CVE-2020-1648 - CVE-2020-1647
CVE-2020-1646 - CVE-2020-1644 - CVE-2020-1654
CVE-2020-1641 - CVE-2020-1645 - CVE-2020-1640
CVE-2020-1643
Múltiples vulnerabilidades (1)
CVE-2020-4274 - CVE-2017-3164 - CVE-2020-4294
CVE-2019-2989 - CVE-2019-2975 - CVE-2019-2981
CVE-2019-2973 - CVE-2019-2964 - CVE-2019-4593
CVE-2020-4272 - CVE-2020-4270 - CVE-2020-4269
CVE-2019-4594 - CVE-2020-4268 - CVE-2020-4271
CVE-2019-4654 - CVE-2018-0734 - CVE-2019-4508

Fabricante

Juniper

Producto afectado

Juniper Networks Juniper Secure Analytics (JSA), versiones 3.0, 3.1, 3.2 versiones anteriores a 7.3.2 Patch 7, 3.3 versiones anteriores a 7.3.3 Patch 3.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00268-01/
https://www.csirt.gob.cl/media/2020/07/9VSA20-00268-01.pdf

CSIRT advierte de vulnerabilidad en Zoom para Windows	
Alerta de seguridad cibernética	9VSA20-00269-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 de Julio de 2020
CVE	
Vulnerabilidad de día cero en el software de videoconferencia Zoom para Windows que podría permitir a un atacante ejecutar código arbitrario en la computadora de una víctima con Microsoft Windows 7 o anterior.	
Fabricante	
Zoom	
Producto afectado	
Todas las versiones del cliente Zoom anteriores a la versión 5.1.3 (28656.0709) que se utilicen en Windows 7 o versiones anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00269-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00269-01.pdf	

CSIRT comparte actualizaciones de Microsoft de Martes de Parche		
Alerta de seguridad cibernética		9VSA20-00270-01
Clase de alerta		Vulnerabilidad
Tipo de incidente		Sistema y/o Software Abierto
Nivel de riesgo		Alto
TLP		Blanco
Fecha de lanzamiento original		14 de Julio de 2020
Última revisión		14 de Julio de 2020
CVE		
ADV200008	CVE-2020-1350	CVE-2020-1433
CVE-2020-1032	CVE-2020-1351	CVE-2020-1439
CVE-2020-1036	CVE-2020-1358	CVE-2020-1442
CVE-2020-1040	CVE-2020-1361	CVE-2020-1445
CVE-2020-1041	CVE-2020-1367	CVE-2020-1446
CVE-2020-1042	CVE-2020-1386	CVE-2020-1447
CVE-2020-1043	CVE-2020-1389	CVE-2020-1448
CVE-2020-1147	CVE-2020-1391	CVE-2020-1449
CVE-2020-1240	CVE-2020-1397	CVE-2020-1458
CVE-2020-1330	CVE-2020-1419	CVE-2020-1461
CVE-2020-1342	CVE-2020-1420	CVE-2020-1462
CVE-2020-1346	CVE-2020-1426	CVE-2020-1349
CVE-2020-1432		
Vulnerabilidades adicionales informadas		
CVE-2020-1025	CVE-2020-1381	CVE-2020-1416
CVE-2020-1085	CVE-2020-1382	CVE-2020-1418
CVE-2020-1249	CVE-2020-1384	CVE-2020-1421
CVE-2020-1267	CVE-2020-1385	CVE-2020-1422
CVE-2020-1326	CVE-2020-1387	CVE-2020-1423
CVE-2020-1333	CVE-2020-1388	CVE-2020-1424

CVE-2020-1336	CVE-2020-1390	CVE-2020-1425
CVE-2020-1344	CVE-2020-1392	CVE-2020-1427
CVE-2020-1347	CVE-2020-1393	CVE-2020-1428
CVE-2020-1352	CVE-2020-1394	CVE-2020-1429
CVE-2020-1353	CVE-2020-1395	CVE-2020-1430
CVE-2020-1354	CVE-2020-1396	CVE-2020-1431
CVE-2020-1355	CVE-2020-1398	CVE-2020-1434
CVE-2020-1356	CVE-2020-1399	CVE-2020-1435
CVE-2020-1357	CVE-2020-1400	CVE-2020-1436
CVE-2020-1359	CVE-2020-1401	CVE-2020-1437
CVE-2020-1360	CVE-2020-1402	CVE-2020-1438
CVE-2020-1362	CVE-2020-1403	CVE-2020-1441
CVE-2020-1363	CVE-2020-1404	CVE-2020-1443
CVE-2020-1364	CVE-2020-1405	CVE-2020-1444
CVE-2020-1365	CVE-2020-1406	CVE-2020-1450
CVE-2020-1366	CVE-2020-1407	CVE-2020-1451
CVE-2020-1368	CVE-2020-1408	CVE-2020-1454
CVE-2020-1369	CVE-2020-1409	CVE-2020-1456
CVE-2020-1370	CVE-2020-1410	CVE-2020-1457
CVE-2020-1371	CVE-2020-1411	CVE-2020-1463
CVE-2020-1372	CVE-2020-1412	CVE-2020-1465
CVE-2020-1373	CVE-2020-1413	CVE-2020-1469
CVE-2020-1374	CVE-2020-1414	CVE-2020-1481
CVE-2020-1375	CVE-2020-1415	

Fabricante

Microsoft

Producto afectado

.NET Core 2.1
.NET Core 3.1
Azure DevOps Server 2019
Azure Storage Explorer
Bond 9.0.1
Internet Explorer 9, 11
Microsoft .NET Framework
0 Service Pack 2
0 Service Pack 2
5
5 y 4.6.2/4.7/4.7.1/4.7.2
5 y 4.6/4.6.1/4.6.2
5 y 4.7.1/4.7.2
5 y 4.7.2
5 y 4.8
5.1
5.2
6
6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
8
Microsoft 365 Apps for Enterprise (32-bit y 64-bit)
Microsoft Bing Search for Android
Microsoft Edge (EdgeHTML-based)
Microsoft Forefront Endpoint Protection 2010

Microsoft Lync Server 2013
Microsoft Office
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
2016 for Mac
2019 (32-bit y 64-bit editions)
2019 for Mac
Online Server
Web Apps 2013 Service Pack 1
Web Apps 2010 Service Pack 2
Microsoft Outlook
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit edition)
Microsoft Project
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
Microsoft Security Essentials
Microsoft SharePoint
Enterprise Server 2013 Service Pack 1
Enterprise Server 2016
Foundation 2013 Service Pack 1
Server 2010 Service Pack 2
Server 2019
Microsoft System Center
2012 Endpoint Protection
2012 R2 Endpoint Protection
Endpoint Protection
Microsoft Visual Studio
2015 Update 3
2017 version 15.9 (incluidos 15.1 – 15.8)
2019 version 16.0
2019 version 16.4 (incluidos 16.0 – 16.3)
2019 version 16.6 (incluidos 16.0 – 16.5)
Code ESLint extension
Microsoft Word
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 Service Pack 1 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
OneDrive for Windows
Skype for Business Server
2015 CU 8
2019 CU2
TypeScript
Visual Studio Code
Windows 10

Version 1607, 1709, 1803, 1809, 1903, 1909, 2004, para 32 bit, 64 bit y ARM64-based Windows 7 32-bit Systems Service Pack 1 x64-based Systems Service Pack 1 Windows 8.1 32-bit systems x64-based systems Windows Defender Windows RT 8.1 Windows Server 2008 32-bit Systems Service Pack 2 32-bit Systems Service Pack 2 (Server Core installation) Itanium-Based Systems Service Pack 2 x64-based Systems Service Pack 2 x64-based Systems Service Pack 2 (Server Core installation) R2 for Itanium-Based Systems Service Pack 1 R2 for x64-based Systems Service Pack 1 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 2012 Server Core installation R2 y R2 (Server Core installation) Windows Server 2016 2016 Server Core installation Windows Server 2019 2019 Server Core installation Windows Server version 1903 (Server Core installation) version 1909 (Server Core installation) version 2004 (Server Core installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00270-01/
https://www.csirt.gob.cl/media/2020/07/9VSA20-00270-01.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
190.147.137.153	Malware	192.241.224.37	Port Scan
181.211.130.109	Malware	192.241.229.157	Port Scan
190.3.183.19	Malware	192.241.212.230	Port Scan
190.3.183.18	Malware	45.143.220.30	Port Scan
92.223.93.153	Malware	205.185.123.45	Port Scan
181.199.102.179	Malware	45.143.220.30	Port Scan
66171248178	Malware	192.241.216.161	Port Scan
104.152.52.22	Port Scan	192.241.212.195	Port Scan
80.82.77.3	Port Scan	192.241.234.68	Port Scan
94.102.56.216	Port Scan	185.36.81.92	Port Scan
199.19.225.202	Port Scan	192.241.214.172	Port Scan
205.185.114.116	Port Scan	192.241.214.52	Port Scan
158.69.107.28	Port Scan	192.241.236.94	Port Scan
72.167.226.94	Port Scan	192.241.210.121	Port Scan
192.241.211.204	Port Scan	188.165.4.153	Port Scan
91.236.116.38	Port Scan	156.96.59.63	Port Scan
91.240.118.64	Port Scan	45.143.220.63	Port Scan
93.174.93.139	Port Scan	192.241.228.15	Port Scan
45.143.220.65	Port Scan	192.241.234.142	Port Scan
185.92.73.230	Port Scan	209.59.154.141	Port Scan
195.62.46.69	Port Scan	192.241.214.162	Port Scan
192.241.236.146	Port Scan	192.241.230.64	Port Scan
89.144.47.244	Port Scan	198.199.107.65	Port Scan
192.241.234.126	Port Scan	192.241.212.93	Port Scan
93.174.93.231	Port Scan	192.241.228.121	Port Scan
185.39.10.92	Port Scan	51.158.27.21	Port Scan
45.125.65.32	Port Scan	192.241.225.114	Port Scan
37.49.224.153	Port Scan	192.241.216.111	Port Scan
78.128.113.42	Port Scan	79137116226	Port Scan
207.244.92.4	Port Scan	192.241.234.141	Port Scan

207.244.92.3	Port Scan	206.81.7.1	Port Scan
192.241.211.219	Port Scan	192.241.234.241	Port Scan
192.241.212.32	Port Scan	198.199.94.50	Port Scan
185.92.220.111	Port Scan	51.15.55.53	Port Scan
157.52.193.99	Port Scan	192.241.233.93	Port Scan
103.232.39.241	Port Scan	192.241.233.246	Port Scan
157.52.193.70	Port Scan	63.143.35.82	Port Scan
150.109.167.155	Port Scan	192.241.236.40	Port Scan
157.52.193.122	Port Scan	103.253.42.61	Port Scan
89.248.174.203	Port Scan	45.148.10.114	Port Scan
192.241.210.32	Port Scan	185.53.91.80	Port Scan
156.96.114.102	Port Scan	192.241.212.209	Port Scan
192.241.212.26	Port Scan	185.222.59.29	Port Scan
207.244.70.51	Port Scan	192.241.230.128	Port Scan
193.6.57.109	Port Scan	185.53.88.236	Port Scan
129.227.129.162	Port Scan	175.183.22.55	Port Scan
192.241.217.80	Port Scan	192.241.217.10	Port Scan
190.105.229.21	Port Scan	178.32.105.40	Port Scan
168.196.255.50	Port Scan	198.50.195.104	Port Scan
192.241.230.73	Port Scan	185.200.118.51	Port Scan
192.241.216.161	Port Scan	178.170.111.34	Port Scan
192.241.214.65	Port Scan	185.216.140.240	Port Scan
192.241.236.64	Port Scan	192.241.234.7	Port Scan
198.199.107.107	Port Scan	192.241.211.193	Port Scan
192.241.236.171	Port Scan	103.125.190.54	Port Scan
212.83.181.11	Port Scan	205.185.114.226	Port Scan
5.35.254.142	Port Scan	37.49.224.159	Port Scan
157.52.193.67	Port Scan	192.241.233.119	Port Scan
150.109.229.30	Port Scan	180.211.162.114	XSS
157.52.193.81	Port Scan	139.255.87.234	XSS
157.52.193.81	Port Scan	154.79.246.178	XSS
93.174.89.53	Port Scan	45.188.120.64	XSS
157.52.193.67	Port Scan	186.208.5.42	XSS
194.180.224.3	Port Scan	85.117.61.186	XSS
45.79.189.15	Port Scan	200.54.56.107	XSS
95.214.52.151	Port Scan	45.178.132.9	XSS
193.37.252.18	XSS		

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.

Actualidad

Procedimiento para denunciar suplantación de identidad en Redes Sociales

La usurpación o suplantación de identidad es utilizada con distintos fines, ya sea para cometer actos ilícitos o con el objetivo de acosar a una persona en particular. En ambos casos es considerado un delito y, por lo mismo, los usuarios de las redes sociales pueden denunciar estas conductas.

Si necesitas reportar una cuenta falsa te explicamos el paso a paso de cómo realizar este procedimiento en Facebook, Instagram, Tik Tok y Twitter, ingresando aquí: Procedimiento para denunciar suplantación de identidad en redes sociales

Ver en: https://www.csirt.gob.cl/recomendaciones/procedimiento-para-denunciar-suplantacion-de-identidad-en-redes-sociales/

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.

- Rodrigo Cortés
- Paola Vidal
  Linkedin:
  https://www.linkedin.com/in/paola-v-79124871/
- David Ahumada
  Linkedin:
  https://www.linkedin.com/in/david-ahumada-soto-05465662/
- Nicolás Fernández
  Linkedin:
  https://www.linkedin.com/in/nicolas-fernandez-6415b377/
- Claudia Lillo
  Linkedin:
  https://www.linkedin.com/in/claudia-andrea-lillo-saffa-a21a4b32/
- Matia Cornejo
  Linkedin:
  https://www.linkedin.com/in/matia-cornejo/

CSIRT Gobierno de Chile Firmado digitalmente por CSIRT Gobierno de Chile Fecha: 2020.07.18 12:39:03 -04'00'