06-08-2020 | Año 2 | N°57

Boletín de Seguridad Cibernética

Semana del 30 de julio al 05 de agosto de 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

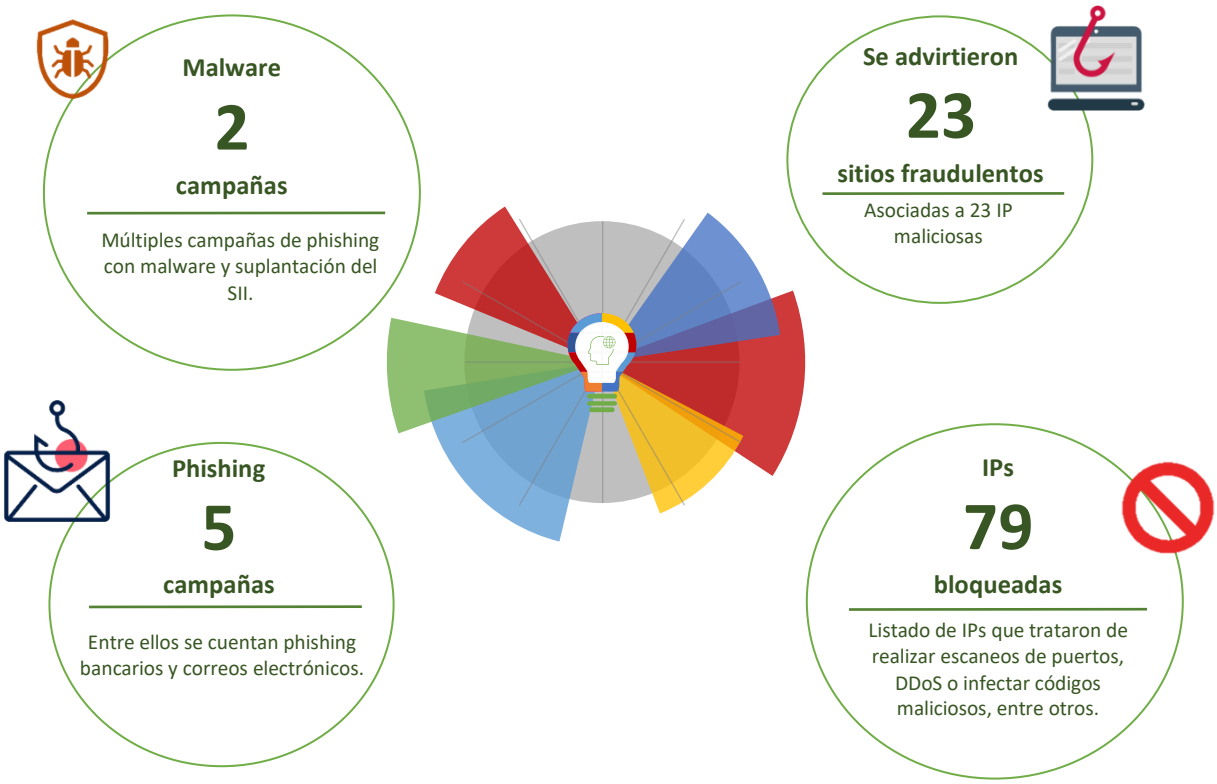
División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras



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

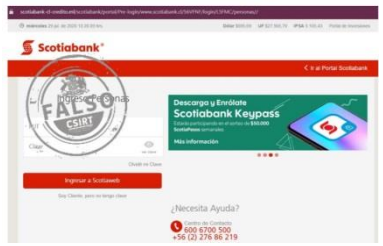
Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00561-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestadocl-portal[.]cf/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0561-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00561-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de suplantación de bancos	
Alerta de seguridad cibernética	8FFR20-00562-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
scotiabank-cl-credito[.]ml/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl/56VFNF/login/L5FMC/personas//	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0562-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00562-01.pdf	

Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00563-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado-app[.]xyz/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]54[.]115[.]153	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0563-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00563-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00564-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
mesjaunos[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
88[.]119[.]179[.]88	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-0564-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00564-01.pdf	

Imagen del sitio

CSIRT advierte de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00565-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
homebchile-smsverify[.]website	
IP	
162[.]0[.]232[.]100	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00565-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00565-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00566-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2020
Última revisión	30 de Julio de 2020
Indicadores de compromiso	
URL	
vpgeles[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
88[.]119[.]179[.]88	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00566-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00566-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00567-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio de 2020
Indicadores de compromiso	
URL	
ndpsghandal[.]com/www[.]bci[.]cl/pagina/index[.]php	
IP	
43[.]225[.]55[.]182	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00567-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00567-01.pdf	

Imagen del sitio

CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00568-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado[.]xyz/bancoestado-banco/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
104[.]219[.]248[.]102	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00568-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00568-01.pdf	

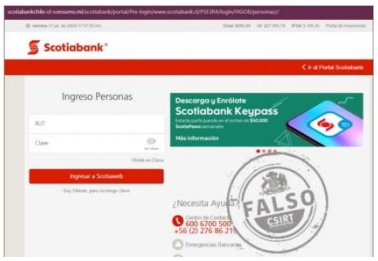
Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00569-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]pci[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
104[.]27[.]143[.]238	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00569-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00569-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00570-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio de 2020
Indicadores de compromiso	
URL	
bancoestado-cl[.]myftp[.]biz/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00570-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00570-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00571-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Agosto de 2020
Última revisión	01 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabankchile-cl-consumo[.]ml/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl/P5E3R4/login/VIGOB/personas//	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00571-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00571-01.pdf	

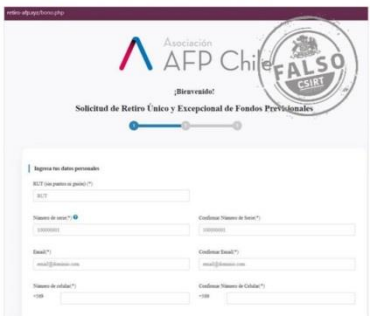
Imagen del sitio

CSIRT advierte de web que suplanta a sitio bancario	
Alerta de seguridad cibernética	8FFR20-00572-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Agosto de 2020
Última revisión	01 de Agosto de 2020
Indicadores de compromiso	
URL	
percontra[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
88[.]119[.]179[.]88	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00572-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00572-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00573-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Agosto de 2020
Última revisión	01 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado[.]app/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
68[.]65[.]122[.]52	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00573-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00573-01.pdf	

Imagen del sitio



CSIRT advierte de sitio que suplanta web de AFP	
Alerta de seguridad cibernética	8FFR20-00574-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Agosto de 2020
Última revisión	01 de Agosto de 2020
Indicadores de compromiso	
URL	
retiro-afp[.]xyz/bono[.]php	
IP	
190[.]107[.]177[.]58	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00574-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00574-01.pdf	

Imagen del sitio

CSIRT advierte sitio fraudulento de plataforma de streaming	
Alerta de seguridad cibernética	8FFR20-00575-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
www[.]netflixfreee[.]ga	
IP	
172[.]217[.]214[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00575-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00575-01.pdf	

Imagen del sitio

CSIRT informa sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00576-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
clientesacceso[.]xyz	
IP	
172[.]67[.]205[.]225	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00576-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00576-01.pdf	

CSIRT informa suplantación de página bancaria	
Alerta de seguridad cibernética	8FFR20-00577-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
personas-bancochile[.]zonanetmovil[.]com	
IP	
174[.]138[.]190[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00577-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00577-01.pdf	

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00578-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
www[.]rnga[.]lt/www[.]santander[.]cl/pagina/login[.]asp	
IP	
88[.]119[.]179[.]88	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00578-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00578-01.pdf	

CSIRT advierte página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00579-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
bancochile-personas-creditos[.]cf	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00579-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00579-01.pdf	

CSIRT advierte sitio falso de empresa de software	
Alerta de seguridad cibernética	8FFR20-00580-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
apple[.]security-id-login[.]com/H/Signin	
IP	
35[.]214[.]219[.]220	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00580-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00580-01.pdf	

CSIRT informa página bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00581-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
scotiabank-cl[.]ga/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl/6MV50Y/login/VNUXG/personas//	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00581-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00581-01.pdf	

CSIRT advierte suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR20-00582-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
bancoestado-movil[.]com[.]de/inicio/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]54[.]114[.]240	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00582-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00582-01.pdf	

Imagen del sitio

CSIRT informa sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00583-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
login-personas-cl[.]bcipass[.]com/1596547836/personas	
IP	
3[.]14[.]27[.]241	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00583-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00583-01.pdf	

Imagen del sitio

CSIRT informa de sitio falso de plataforma de streaming	
Alerta de seguridad cibernética	8FFR20-00584-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
URL	
netflix[.]security-id-login[.]com/app/login	
IP	
35[.]214[.]219[.]220	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00584-01/	
https://www.csirt.gob.cl/media/2020/08/8FFR20-00584-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de phishing bancario por crédito FOGAPE	
Alerta de seguridad cibernética	8FPH20-00276-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2020
Última revisión	31 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://bancoestado-cl-creditos[.]tk	
IP	
178.159.36.76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00276-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00276-01.pdf	

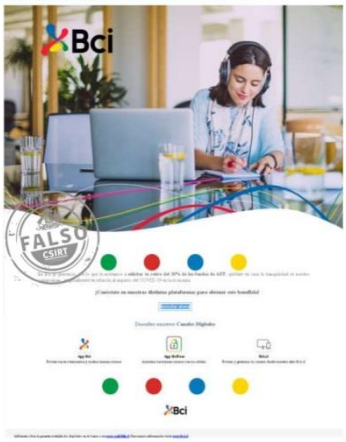
Imagen del mensaje

CSIRT advierte phishing de servicio de streaming	
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	03 de Agosto de 2020
Última revisión	03 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://aqua.nefttlix.sign.rosjaw[.]com/login_cl_8j88/premium/actualiza.php	
IP	
[195.252.110.172]	
[36.255.220.21]	
[82.208.77.27]	
[186.64.19.176]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00277-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00277-01.pdf	

Imagen del mensaje

CSIRT advierte phishing bancario por aumento de cupo	
Alerta de seguridad cibernética	8FPH20-00278-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Agosto de 2020
Última revisión	03 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://bancochile-personas-credito[.]ml/ww3.bancochile.cl/nuevo/www.bancochile.cl/jb9pw5ikp2/dviti_persona/login_ksga/index/login2iq7/}	
IP	
[103.248.146.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00278-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00278-01.pdf	

Imagen del mensaje



CSIRT informa phishing por retiro de AFP	
Alerta de seguridad cibernética	8FPH20-00279-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Agosto de 2020
Última revisión	04 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxp://promo.dorsetthotels[.]com/wp-includes/css/sixhubrsndmoacpupfiuzzfwunbqzupjo/	
hxxps://login-personas-cl.bcipass.com/1596569333/personas#	
IP	
[173.254.64.10]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00279-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00279-01.pdf	

Imagen del mensaje

CSIRT advierte smishing bancario por AFP	
Alerta de seguridad cibernética	8FPH20-00280-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Agosto de 2020
Última revisión	04 de Agosto de 2020
Indicadores de compromiso	
URL	
hxxps://itau-movil.siteverify.online	
hxxps://banca-itau.verify-sitecl[.]com/1596573333/bancochile-web/persona/login/index.html/login	
IP	
66.23.230.67	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00280-01/	
https://www.csirt.gob.cl/media/2020/08/8FPH20-00280-01.pdf	

Malware

CSIRT advierte múltiples campañas de phishing con malware	
Alerta de seguridad cibernética	2CMV20-00069-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
Indicadores de compromiso	
17 tipos de hash	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00069-01/	
https://www.csirt.gob.cl/media/2020/08/2CMV20-00069-01.pdf	

CSIRT advierte malware que suplanta al SII	
Alerta de seguridad cibernética	2CMV20-00070-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Agosto de 2020
Última revisión	05 de Agosto de 2020
URL	
hxxps://takarada-lab.ees.st.gunma-u.ac[.]jp/website/wp-content/themes/twentynineteen/classes/000012989018087978947891287312891TR/index1.php	
hxxp[:]//wwwfox.supremetearmazenfoxweb[.]com/tr/	
Indicadores de compromiso	
12 tipos de hash	
26 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00070-01/	
https://www.csirt.gob.cl/media/2020/08/2CMV20-00070-01.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
45.148.120.13	Malware	192.241.236.133	Port Scan
151.237.16.5	Malware	45.148.121.77	Port Scan
198.57.203.63	Malware	199.19.226.115	Port Scan
115.165.3.213	Malware	164.90.189.77	Port Scan
177.37.81.212	Malware	129.227.129.166	Port Scan
144.139.91.187	Malware	45.95.168.217	Port Scan
206.212.248.178	Malware	192.241.234.4	Port Scan
181.164.110.7	Malware	192.241.230.18	Port Scan
181.134.9.162	Malware	147.75.34.138	Port Scan
89.108.158.234	Malware	112.140.185.246	Port Scan
181.143.101.19	Malware	168.121.97.162	Port Scan
46.49.124.53	Malware	164.68.111.85	Port Scan
190.111.215.4	Malware	62.210.139.120	Port Scan
144.139.91.187	Malware	192.99.44.2	Port Scan
191.238.222.184	Malware	93.174.89.43	Port Scan
133.8.136.19	Malware	192.241.219.24	Port Scan
124.146.197.23	Malware	148.72.158.112	Port Scan
104.47.55.110	Malware	141.98.10.141	Port Scan
49.45.28.21	Port Scan	103.145.12.21	Port Scan
185.39.11.53	Port Scan	173.249.29.113	Port Scan
38.91.107.152	Port Scan	156.96.128.163	Port Scan
208.113.157.101	Port Scan	45.148.10.12	Port Scan
208.113.157.103	Port Scan	192.241.236.125	Port Scan
66.33.200.148	Port Scan	172.241.213.94	Port Scan
45.148.120.13	Port Scan	138.99.224.220	Port Scan
141.98.10.193	Port Scan	103.207.36.147	Port Scan
45.148.121.63	Port Scan	66.33.200.149	Port Scan
52.252.56.58	Port Scan	128.14.141.102	Port Scan
156.96.128.163	Port Scan	103.114.105.83	Port Scan

103.99.0.24	Port Scan	58.182.171.48	Port Scan
192.241.214.134	Port Scan	116.86.153.61	Port Scan
128.14.141.103	Port Scan	173.212.208.234	Port Scan
88.218.17.37	Port Scan	156.96.58.118	Port Scan
192.241.234.29	Port Scan	203.162.79.194	Port Scan
198.199.101.122	Port Scan	45.148.121.81	Port Scan
192.241.236.167	Port Scan	192.241.234.53	Port Scan
161.97.91.103	Port Scan	128.14.141.104	Port Scan
129.227.129.165	Port Scan	103.207.37.99	Port Scan
37.49.230.232	Port Scan	192.241.214.40	Port Scan
192.241.234.58	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.

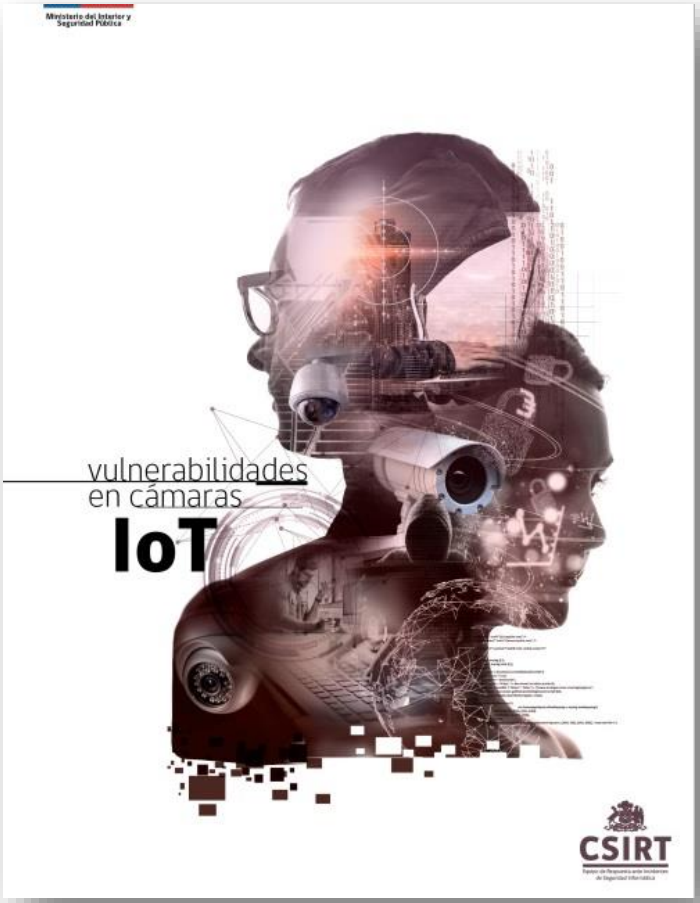
Investigación

Vulnerabilidades en Cámaras IoT

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la décimo tercera edición de su publicación sobre amenazas cibernéticas el que analiza la seguridad en cámaras IoT. Este artículo fue elaborado por Juan Moraga y Natalia Pérez, analistas de CSIRT.

En este artículo nos concentraremos en analizar las vulnerabilidades de los IoT. Para ello se seleccionó a las cámaras de seguridad como dispositivo para ser analizado. La razón de por qué escogemos este dispositivo, es para representar la paradoja del problema de la seguridad cibernética, precisamente en un dispositivo diseñado para resguardar la seguridad, y cómo se puede transformar una herramienta de apoyo en un instrumento de perjuicio.

El trabajo además se completa con una serie de pruebas de concepto (PoC) para probar algunas de las vulnerabilidades encontradas en cámaras web, y una serie de recomendaciones de seguridad para los dispositivos IoC en general, y de cámaras en particular.



Ver más en: https://www.csirt.gob.cl/reportes/an2-2020-13/

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.

- Alberto Rivera
- David Cordovez