19-01-2020 | Año 2 | N°72

Boletín de Seguridad Cibernética

Semana del 12 al 18 de Noviembre de 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.

Gobierno de Chile

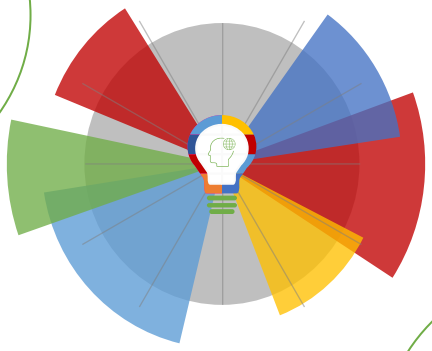
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras

Hash
58
Sha 256
Asociadas a múltiples campañas de phishing son archivos que contienen malware

Se advirtieron
13
URLs
Asociadas a sitios fraudulentos y múltiples campañas de phishing y malware



Parches
36
para vulnerabilidades
Las mitigaciones son útiles para productos Windows, Chrome, WhatsApp y Samba.

IPs
155
Informadas
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte de sitio que suplanta a portal de pago online	
Alerta de seguridad cibernética	8FFR20-00826-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2020
Última revisión	13 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//glassfilm[.]cl/wp-admin/webapp/update/	
IP	
190[.]107[.]177[.]239	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00826-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00826-01.pdf	

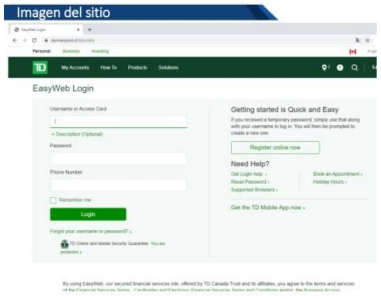
Imagen del sitio

CSIRT advierte de sitio que suplanta a sitio bancario internacional	
Alerta de seguridad cibernética	8FFR20-00827-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Noviembre de 2020
Última revisión	14 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//nutricionyterapias[.]cl/.ch./ch/auth/log.php	
IP	
190[.]107[.]177[.]232	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00827-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00827-01.pdf	

CSIRT advierte de portal que suplanta a página de inicio de red social	
Alerta de seguridad cibernética	8FFR20-00828-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Noviembre de 2020
Última revisión	14 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//set-87402714.elsenordelosbajones[.]cl/gate.html?location=d304f7bf638d833842098a893ae76605	
IP	
190[.]107[.]177[.]232	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00828-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00828-01.pdf	

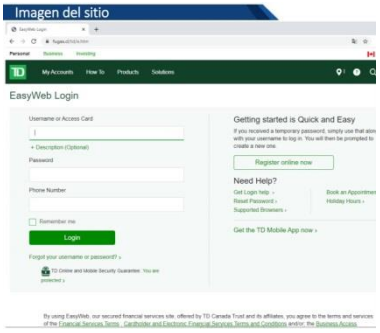
CSIRT informa sobre sitio que suplanta a web financiera global	
Alerta de seguridad cibernética	8FFR20-00829-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Noviembre de 2020
Última revisión	14 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//cortinasrollerazteca[.]cl/ww/secure.connect/auth.present/ea037c6e33582d13b5b71f516a8b261f/First-page/	
IP	
200[.]32[.]181[.]200	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00829-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00829-01.pdf	

CSIRT advierte de sitio que suplanta a banco	
Alerta de seguridad cibernética	8FFR20-00830-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//migasfiter[.]cl/td/e.htm	
IP	
[201.148.107.69]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00830-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00830-01.pdf	



CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00831-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//www.dunnerpool[.]cl/td/e.htm	
IP	
[201.148.107.69]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00831-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00831-01.pdf	

Imagen del sitio



CSIRT informa sobre portal de banco fraudulento	
Alerta de seguridad cibernética	8FFR20-00832-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//www.fugas[.]cl/td/e.htm	
IP	
[201.148.107.69]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00832-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00832-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00833-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//avancefecitivobancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
186.64.118.235	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00833-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00833-01-1.pdf	

Phishing

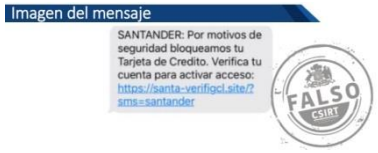
Imagen del mensaje

CSIRT advierte de phishing bancario por verificación de cuenta	
Alerta de seguridad cibernética	8FPH20-00326-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Noviembre de 2020
Última revisión	10 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//cmmila6[.]pl/cli/enviar.php?l=812122543	
https[:]//sartoriafragomeni[.]it/frag/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[45.7.231.143]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00326-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00326-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por reactivación de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00327-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//santander.personascl[.]site/1605527542/index.asp	
IP	
[69.167.167.190]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00327-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00327-01.pdf	

Imagen del mensaje



CSIRT advierte de smishing por bloqueo de tarjeta	
Alerta de seguridad cibernética	8FPH20-00328-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre de 2020
Indicadores de compromiso	
URL	
https://santa-verifigcl[.]site/?sms=santander	
https://smsapp-santacl[.]xyz/1605529755/personas/index.asp	
IP	
162.0.235.141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00328-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00328-01.pdf	

Vulnerabilidades

CSIRT comparte información de vulnerabilidades obtenidas de Google	
Alerta de seguridad cibernética	9VSA20-00320-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre de 2020
CVE	
CVE-2020-16016 - CVE-2020-16013 - CVE-2020-16017	
Fabricante	
Google	
Productos afectados	
Google Chrome para Android versiones anteriores a la 86.0.4240.193. Google Chrome para Android versiones anteriores a la 86.0.4240.198.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00320-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00320-01.pdf	

CSIRT comparte mitigaciones para vulnerabilidades obtenidas de Moodle	
Alerta de seguridad cibernética	9VSA20-00321-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Noviembre de 2020
Última revisión	05 de Noviembre de 2020
CVE	
CVE-2020-25627 - CVE-2020-25628 - CVE-2020-25629 CVE-2020-25630 - CVE-2020-25631 - CVE-2020-25698 CVE-2020-25699 - CVE-2020-25700 - CVE-2020-25701 CVE-2020-25702 - CVE-2020-25703	
Fabricante	
Moodle	
Productos afectados	
La vulnerabilidad afecta a Moodle entre la versión 3.9 y la 3.9.1. La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7, 3.5 y la 3.5.13. La vulnerabilidad afecta a Moodle entre las versiones 3.9 y la 3.9.1, 3.8 y la 3.8.4, 3.7 y la 3.7.7, 3.5 y la 3.5.13 y versiones anteriores sin soporte.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00321-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00321-01.pdf	

CSIRT comparte mitigaciones para 21 vulnerabilidades de Cisco	
Alerta de seguridad cibernética	9VSA20-00322-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020
CVE	
Críticas: CVE-2020-3531 - CVE-2020-3586 - CVE-2020-3470 **Altas:** CVE-2020-3392 - CVE-2020-26072 - CVE-2020-3367 CVE-2020-3284 - CVE-2020-27131 **Medias:** CVE-2020-3482 - CVE-2020-26077 - CVE-2020-26078 CVE-2020-26079 - CVE-2020-26075 - CVE-2020-26076 CVE-2020-26080 - CVE-2020-26081 - CVE-2020-26068 CVE-2020-3419 - CVE-2020-3471 - CVE-2020-3441 CVE-2020-27126 - CVE-2020-27131	
Fabricante	
Cisco	
Productos afectados	
Estas vulnerabilidades afectan a las versiones 4.22 y anteriores de Cisco Security Manager. En el momento de la publicación, esta vulnerabilidad afectaba a Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) que ejecutaban una versión de software anterior a la versión X12.6.3. En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00322-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00322-01.pdf	

IoC - Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos
e67fdd41896f179eb8a8e33171011687a75d64149a2b9d70e418a56702d8037f
fe51cfe8bfebd7912fab5269ba2f2f8bed2b455045d0e6de78cee6e05d090606
e6c9a39863fe8541b4a57b54fd2fd342de4c8246c19798e7a1d25f5ab6d7b7f0
70d2867c766b54c413360ee05632ef75f5dd67d414dfdb23a1eb5d7831ef2681
e35022da0ce64e1fa71838f4db5344ccb9d432065ae01a6ef6f50f8437645ab1
4983bd5fd9e1316ddc152720390bfa6ca83de9493eb0f12d76fa585f3795ffa7
bbe85d35d87417aaddee6aefc5701dfe76fe7b22b9fe2d675c50e33a67ee4fef
6116d689621dbb133b8aa118c9f777044ff3416ff57d83e4ed3fa5310cfaef25
ecb448d3b0c7d86ffc87e6c8a073bce412e7767826bf505ec4d26b9f799100dc
30de7b26e71dfa42859f03eedd475c8b38b2c453e0a8c7ed1e8417412317c7c6
337c613260fcc3e6a106da88bc60f99d9079116f2094085ac5cb8b497b819e2c
65fd502b8dbe07244adc4b956bd77eb077652f011ec6d55c65cde8edd623e8d4
c89a4ae21bc0aca7e57261ec4c0b4c3f4607167bc400e62ba4b09416c8bbf148
3d0495416c10ec60cdd0aa9189d519d516b6caee2d77e7458175113b74d78b34
c0de23b56e1fe15356f009ff76a214fe35f0c265838220bac2034e18816bffae
0f1fc79048538455989cb13006fc8f04838baaf649f942b5822639e02855fe59
b51e68a52d085aeec83086f3763c7fc12747b8123ee8227eb780a38cf2e2062e
a503b07c67997fa3f2ddc0d2d98bc9660268b99d13f6ab09ac39a000d4889754
68230ef6e3efc29eea5bbd5dab1c8ca4de9df2598b8f9156fb8ebc0a5bbf23dc
6172434eb1ad5c668f2470ad07d3e3e015455fef4451f712eb5e29c7a5d2b205
fca4f23dee3ae9b5ef4e4d2ff8711ada04591ca316217d34011d815dfa43ba9a
e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887
21ce7c7809b66a85c380b9131843a246098c51a1da43df3adc2bf4b6698620c2
d81bd9b51d9746aa98406f9c05c5b70d8c14a5235b78ff847d6a3fbc18feb129
5aa66e468b69c5c39744ac23da7affc929f579fa31c10e32b2e8c7142b660aa9
cb316023b967173374bcf1ff23a0a9d0abafc6ae392400eae0c517a779ae9e3a
9c90e683f72057ea25f5281223c16b56cb3a20d358772d6b5ffe1802a10ba11d
c674034c60787e367d74a1dc8458920cfc2ba0f06dc4ab97178f8ead652af9cb
06f543b439a6b9f7f435cb03a5eab6e5a310719e5e47d518af554d317072ba64
ad146fbb6f2e0bd2e0fab014d9fffc16b5d05517bcb5f765713afab2ad3316ab
06f543b439a6b9f7f435cb03a5eab6e5a310719e5e47d518af554d317072ba64

1f85630cfa677de440f8923d2924c1420d63be4dddab5a4e31c40abc895ab9d4
7df5580d18907280fa51377b6d55a3188a2e396cc49fa0815859df8a63fe86be
da81bb17be325dea97eedb4dc5f91b153202fe7d220a620aa7b0253aaba5129c
07f6615ee0145771ca149c49196c2a37567b176585a1d4653e9884e55f3d2d54
02509119541d211e419b813f0227ad689da496ad37551e5edc8a8fe91c024751
cb3304eb9d1b5355a16b71678a84be9b4f6d6b966dd721e9e0b1371962df4cc6
6823855ffb97d6e2e64b8801e6ead60d6d0bd51f053c3ab6a59951e01522e999
fda139941faf778a5e9ff87cb2e0028571754fc2f907a4b7f6d0a98eeac52cce
e38ec15fe37a88fd361115f3985f4d898f0ff71897ffe4e91e75f478e3cf7cb7
3eefced73ddd0fc2d2d5e991e0338d795069968ad15d778610f63e14850b8653
bb72fc496c3791609b5f0cd5f2828e4a753c64aa4e3f25f4498f071689621b90
19cf3b870dbc677ebd0701d7677045dbf2ff8ae3ee1d3ede189ef9b19a246e63
cd98e80249695a12bb63e324159ff6abcd6740d4dab3e1da6398d4a4761bf067
d6b43c92cb8982f417b086c5cd11f5d00cc13c5c4d75516cf866add282ec08ae
da17a8157fd775cc9d755800f02339ab63b24aae7347d5f8659ee5702c9c60d0
d8746c76a3a33970bf47cd0c446617c59bccde9aa15499e13a40be7c231eda84
635b5afb2e981d0870b1fba09be3ff6c0a3c823358dff8d055dc1c8a408ac918
45f63b4bbfab4f9d9de18f15e4328950974165ac5053d5f6c2865b06c182ce76
86792bb14cae5863bf4bddc88390330a5a5e7a4db5b580b503fe6615e0456d61
7995b84353dfe51a5b9a5b178e070f3567727798da9e3b7475b9f4c05ed97027
51a879f6c88dacd0c2461a7a1245dea17a5cda7c5d8fd53f53eb682fe813534c
00371e1dee04b9f0ecdb3fbad1beca60559db9bf23343235e89f9146b202ec57
291b86bfb5ba6ba6aa37409ee0854a6b9b60e4107ee62b793cd01c1cc09d9b93
b80759b7d4e4d2e2562d76bbe198948e3a99425957a4991d83233d634c463c03
8d812f90139842e76cd96f8ca50d1d4f7594057c2da04a335c1c6ee4490a2671
c5ffed3b7435b5748a7885bd66997b39a452943b8d2e0f7a2131cd42484c0b26
579f905ac1ab7292d87cbe30e0765bd0e982bbe646905e7ad0d773137e878020

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

82.114.162.38
23.238.48.117
203.124.39.163
103.99.1.172
203.124.39.163
190.145.77.219
185.222.57.252
72.52.244.66

88.218.16.246
88.218.16.246
74.208.120.53
68.66.241.149
74.208.120.53
88.218.16.194
185.222.58.118
172.98.201.44
64.227.65.86
81.42.224.67
81.42.224.67
45.137.22.50
45.137.22.134
45.137.22.75
199.96.83.10
64.227.65.86
185.222.58.102
155.94.136.228
139.59.255.39
188.119.148.113
23.101.174.3
202.63.244.174
40.107.74.80
23.81.246.242
88.218.16.126
37.228.184.136
104.255.168.181
37.49.225.107
103.109.37.72
179.43.176.193
176.123.7.141
80.65.91.214
133.130.121.44
156.96.156.212

Correos electrónicos de donde son enviados los archivos adjunto con malware

a-m-wahlstrom@abbeytitle.com
tech@lyship.com
personnel@technosteel-uae.com
prvs=05820a4f30=Watania@yemen.net.ye
teresa.seguei@floramatic.com
atiqa@rdlpk.com
jimmy.leatherbank@gmail.com
atiqa@rdlpk.com
purchases@vnkc.com
iqra@gifaconsulting.com
ops.pakistan@gac.com
ops.pakistan@gac.com
vipechi@gmail.com
In.tntimportclearance@tnt.com
h.valdes@maiconmetal.cl
operation@platinship.net
matt.williams@newfacultymajority.info
aabros@aabrosgroup.com
chanpitou.acc@widegatetrans.com
elopez@apiassa.com
logistic@bellstone.in
rgsfv@hotmail.com
carvi@sumi.es
sales@supplyafrica.co.tz
oliviahaendra@oil-gas.com
adriannaameida206@gmail.com
fzat@chevorn.com
jarrie.lu@huiliansh.com
arasheedu@yhdo.org
jw61@rnd.re.kr
rasheeddada234@gmail.com
customer@dhl.com
dhiraj.gupta@batas.com
DEAOLIVEIRA@voegol.com.br
wgajelonia@cdmlight.com
info@armatorshipping.com
accounts@cpanel.net

shenwei@sva-int.com
jvgeest@introcare.nl
admin@getemails.site
atg@encomix.es
a-m.stalder@abcdata.com.pl
chouchne0613@gmail.com
zakupy@breve.pl
studenti@unbi.ba
admin@jetmails.fun
renz@rise.qa

IoC - Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

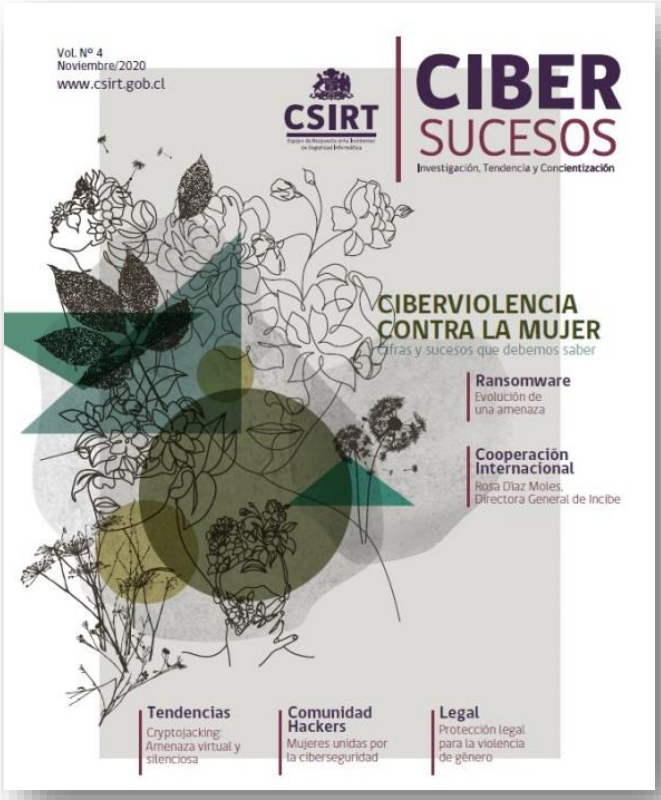
IP		
1.225.101.152	178.254.171.89	37.99.250.11
14.164.136.176	178.254.179.49	37.99.253.141
14.169.193.239	181.176.222.68	37.99.255.113
37.221.178.155	185.100.13.251	37.99.255.176
37.221.179.146	185.246.8.189	41.193.22.146
37.221.179.206	185.246.8.190	58.221.42.231
60.174.118.123	185.246.8.197	58.221.44.163
81.250.162.238	185.246.9.19	59.57.253.66
97.104.206.212	185.39.25.124	60.29.197.152
103.141.138.120	185.49.168.32	61.19.246.25
111.224.166.214	185.92.194.60	69.144.99.202
141.105.104.170	186.31.118.76	77.109.177.12
141.105.105.222	187.84.18.223	83.209.236.79
178.254.171.130	188.255.132.13	94.200.172.30
178.254.171.173	188.255.132.35	175.126.84.168
182.189.201.233	188.255.132.53	177.47.140.133
186.190.224.116	188.255.237.62	177.87.212.234
188.255.131.167	190.86.37.170	118.121.41.19
188.255.131.232	193.169.252.60	121.200.88.226
188.255.131.236	197.237.161.13	122.7.216.73
188.255.132.115	197.237.243.68	123.27.174.100
188.255.132.119	2.186.53.137	125.117.28.184
188.255.132.125	202.134.118.30	134.90.250.91
188.255.132.211	202.165.236.71	134.90.252.156
188.255.237.163	212.69.22.121	134.90.253.173
188.255.237.189	212.69.24.59	14.177.59.181
188.255.237.234	218.25.31.150	14.48.200.79
200.216.159.230	218.82.119.170	141.98.80.79
213.108.162.237	220.233.4.53	154.0.53.50

220.179.231.250	221.3.236.94	156.96.44.183
1.52.160.220	222.138.10.46	156.96.56.184
110.16.85.62	222.141.18.29	168.121.72.148
110.39.184.42	222.223.56.116	171.242.233.29
111.224.166.20	222.67.113.123	175.117.79.125
111.224.166.30	24.209.64.71	37.221.181.31
114.108.125.98	27.128.193.90	114.95.146.116

Actualidad

Cibersucesos n°4

En la cuarta edición de Cibersucesos, CSIRT aborda en su tema principal la violencia de género a través de los distintos canales digitales. Esto, con el objetivo de conmemorar el Día Internacional de la Eliminación de la Violencia contra la Mujer que fue declarado por la ONU con fecha 25 de noviembre. En esta misma línea, en la sección "Legal" hablaremos sobre los avances legislativos en esta materia, como por ejemplo, la Ley Gabriela y un proyecto de ley que busca asegurar el derecho de las mujeres a una vida libre de violencia. En "Comunidad Hackers" les presentaremos a la "Comunidad de Mujeres en Ciberseguridad" y "Comunidad Lovelace", dos grupos compuestos por mujeres que buscan promover y potenciar la ciberseguridad a través de distintas acciones. Por otra parte, quisimos profundizar un tema muy común hoy en día y que ha dado mucho que hablar: el Ransomware. En esta edición de Cibersucesos explicaremos su origen y cómo podemos estar preparados para prevenir este ciberataque. Otra amenaza que está dando que hablar y que podrán leer en la sección "Tendencia Digital" es el Cryptojacking y que también busca obtener una ganancia económica, pero esta vez lo hace para obtener criptomedas.



Ver más: https://www.csirt.gob.cl/recomendaciones/revista-cibersucesos-n4/

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos públicos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Osvaldo Carrasco
- Lukas Lee

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.20 12:24:33 -03'00'