Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

09-04-2021 | Año 3 | N°92

Boletín de Seguridad Cibernética

Semana del 01 al 08 de abril de 2021

La semana en cifras

Hash

69

SHA

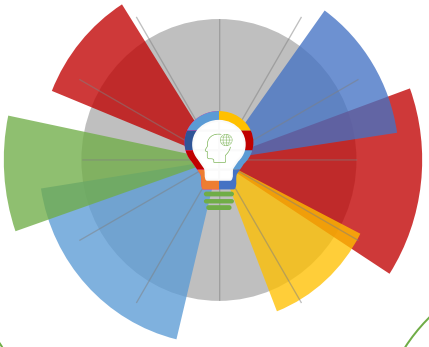
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

13

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

2

para vulnerabilidades

Las mitigaciones son útiles para productos de XX

IP

40

Informadas

Listado de IP 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

Malware

Imagen del mensaje

CSIRT alerta por campaña de malware Agent Tesla, difundida a través de falsos emails de DHL	
Alerta de seguridad cibernética	2CMV21-00164-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de abril de 2021
Última revisión	8 de abril de 2021
Indicadores de compromiso	
SHA256	
E0DBB2C8E0E0C6B0AE425C16DB22614E680591C5FD0D8E7686294CC971FFD42D 440E1D1133BC11666F4D7662493D94FFB8D8C60DCDD683B687104F07051F897A	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00164-01/	

Phishing

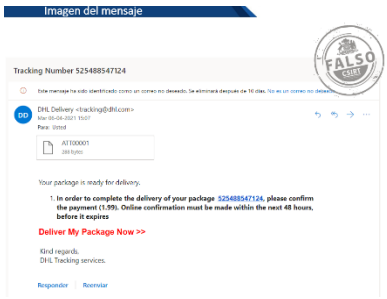
CSIRT alerta ante campaña de phishing con falso email del Banco Santander	
Alerta de seguridad cibernética	8FPH21-00382-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2021
Última revisión	1 de abril de 2021
Indicadores de compromiso	
URL sitio falso	
hxxp://134.209.151.14/1617031307/index.asp	
IP	
[134.209.151.14]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00382-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00382-01.pdf	

CSIRT alerta ante campaña de phishing con falso email de Fonasa	
Alerta de seguridad cibernética	8FPH21-00383-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2021
Última revisión	1 de abril de 2021
Indicadores de compromiso	
URL redirección	
https://tinyurl[.]com/xdnbcu96 https://cdf21-fonasa.blogspot[.]com/	
URL sitio falso	
http://wp1.webmaster-amazon.ndzjp.spectrum.myjino[.]ru/workspaci/moon/po/176b9f1b235b6fab6c37d9709cae1fc0/	
IP	
[81.177.135.150]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00383-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00383-01.pdf	

Imagen del mensaje	CSIRT alerta ante campaña de phishing con falso email del BancoEstado	
	Alerta de seguridad cibernética	8FPH21-00384-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	5 de abril de 2021
	Última revisión	5 de abril de 2021
	Indicadores de compromiso	
	URL redirección	
	http://citypawn[.]ca/sucursal/promo-utig/	
	URL sitio falso	
	https://palestineadvocacy[.]com/metns/imagenes/comun2008/banca-en-linea-personas.html	
	IP	
	[107.180.51.13]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph21-00384-01/	
	https://www.csirt.gob.cl/media/2021/02/8FPH21-00384-01.pdf	

Imagen del mensaje	CSIRT alerta ante campaña de phishing con falso email de Netflix	
	Alerta de seguridad cibernética	8FPH21-00385-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	5 de abril de 2021
	Última revisión	5 de abril de 2021
	Indicadores de compromiso	
	URL redirección	
	http://chechu.mandril.avnam[.]net/wp-content/plugins/preferred-languages/inc/PPPTTXXXMMMMLLLHHTHTTAA.html	
	URL sitio falso	
	https://lightcloud[.]com/wp-includes/JEVAISOPENMYOWAMENFRH/e8f4f4de9c9b93b6898cfdf4af5c6cd1/	
	IP	
	[52.88.172.134]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph21-00385-01/	
	https://www.csirt.gob.cl/media/2021/02/8FPH21-00385-01.pdf	

CSIRT alerta ante campaña de phishing con falso email del Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00386-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de abril de 2021
Última revisión	6 de abril de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3sRmgOH?l=www.bancoripley.cl	
URL sitio falso	
http://bancoripley.cl.deejayteam.com[.]tr/login https://www.chsj[.]in/wp-content/web/BancoRipley.png	
IP	
[185.52.231.246]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00386-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00386-01.pdf	



CSIRT alerta ante campaña de phishing que suplanta a DHL	
Alerta de seguridad cibernética	8FPH21-00387-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2021
Última revisión	7 de abril de 2021
Indicadores de compromiso	
URL redirección	
https://taniaeyanga[.]com/Shipment/Tracking/	
URL sitio falso	
https://taniaeyanga[.]com/Shipment/Tracking/F004f19441/11644210b.php?web=succes&local=_&id=70405351	
IP	
[160.153.131.205]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00387-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00387-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en QNAP QTS	
Alerta de seguridad cibernética	9VSA21-00416-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2021
Última revisión	5 de abril de 2021
CVE	
Ambas vulnerabilidades carecen aún de CVE.	
Fabricante	
QNAP	
Productos afectados	
QNAP QTS con sistemas anteriores a la versión 4.5.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00416-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00416-01.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	Documento web
03f7a319c076292517b055d0344bab973d3386be13ca123f5962c267d6afb516	2CMV21-00163-01
0929f70b8164f9ecc43e2ec56baef3e497a663042935428aafd95dea0a5c9c80	2CMV21-00163-01
0af95bb33b10c1f830b92587e2145e9ae58b750074f7ece5f16ad6d44c96abc9	2CMV21-00163-01
0fbb056128f13b0a290047c7b2edd81ff70a5a5108df588a2a031d6bcccc962b	2CMV21-00163-01
120686ff12e1f3ef4b4e89e8d97a88b141b3611c4d5d7a04181fb00d3c67c8f9	2CMV21-00163-01
192920e2a3dc8de4619016115322cbbc29ac89ed79d4ac331e1c29d2038c2746	2CMV21-00163-01
196e9df7946e1d42d80158a7282520da72a737516c8575a179000d1962542ea0	2CMV21-00163-01
1e4ffff7ac858c089c396daed605ac3a7910082dfc300195663611dbb114ecb6	2CMV21-00163-01
1ef37249de16d48ff222d5b7d63846a9bb3a2ebff07e23241fc3d13e7341d2bf	2CMV21-00163-01
24bb3c90eeafad2dca3d742ad0361e90a38a9cebec3238a24d9ddffad7ef45a6	2CMV21-00163-01
253818f8e55b94a26996a7529583faf9b1d2beaf9953ac3e479e31bf55561f57	2CMV21-00163-01
264c10ad620c793895f9bb5d31dc3911aff88790a8a8d7e59f0c5bf94226c0b9	2CMV21-00163-01
2b6dcd2d9942fe47fd85547211d2822d36551610e8cbec24c1570e3c8bc826c3	2CMV21-00163-01
2dd463937c35210eddced5f4be41e58fd1562a9be3f298693fa1333f75d05c92	2CMV21-00163-01
2e50ab4de171b446fa9d69601142f27defec291c5cccfb55dc20557463c3f92c	2CMV21-00163-01
31ec66e163e5ef9eabf672c13034d5561c162d2e28c4351a45ead3a0bd4b526a	2CMV21-00163-01
32a81b90391f0862db2db6d701ca29772b7c38734f928b302751a8d24d8c4a6b	2CMV21-00163-01
331ed6ea56aff70500a40f195aeb78fbd5fcd86fb000a5300eebba22926f5c36	2CMV21-00163-01
351588c6f208e00c046840524635fdcb6690a4e834e50b04cf29eb739960a556	2CMV21-00163-01
370e2d6aad3b12876fb5d7ce51f7b69438d77f8fa3b6ff9db90ba36591c86fd5	2CMV21-00163-01
3cc300cf3f4442b147736ab4053f9c37007639314555ba204e2e7b5458bdea2e	2CMV21-00163-01
419c60982a5ef28c5a9028bd3ff9dd418dfb9a229f0f672b5cc09865c9212c01	2CMV21-00163-01
45d5b628ea3ebce34feb812984c20b1caaf7ad014744c0d1af92ca4329008d0d	2CMV21-00163-01
49950ea1d80fcd51eb708d70aebde9ec730d3d1157569a32dc4e8d9686635fe4	2CMV21-00163-01
51a0cefbc6f455ae11e414dcfd57b339f49b3728d6e77bf62a2b4dc950ff756c	2CMV21-00163-01
5b400a7336b2386e80d7137462c41d4cb80fb8d80f31474362f966b5bf38c83d	2CMV21-00163-01
5c333ec91c2ea8d08370cf8f0abfa7a92db29a60b2708245419b332324932052	2CMV21-00163-01
5cd2017ab7a8c49f77af32cc17418cebc39caae377be4c6082c76c0ff9dce4b1	2CMV21-00163-01

6131dff0090943da0877cd7eac167190d5cb869b2524757a67bb2f319384f391	2CMV21-00163-01
61a3efa7284be26c128e00f34d4bd4bdedfc2e217997fbf91dec036da78234a4	2CMV21-00163-01
6720a131e0f97d7235f3bb336446b99983010d02a3b86e0e0b6cce427ca92675	2CMV21-00163-01
6abacaf184cab7eec777639ad5b4e4e51a113cb91581eb3eba80f61b5b45b132	2CMV21-00163-01
6c8eedd82cd11a6817482c215333ed36e4d1af232f0690a9f2bb2240deb0b5e2	2CMV21-00163-01
6e449da9cbe233008bd08f5df387a790a3c9edfb0f2beda1b432a17c41a47f15	2CMV21-00163-01
74699899eebe4638fc33dd64adcc4585a4c752e621a3ed7e38abace15621d2f1	2CMV21-00163-01
7554bedfa0e13c1102c7c8609c81a95df21e886a771e5f99016413942b4fbf00	2CMV21-00163-01
79e21293eb53717af3dd983167c1d15f56fc525fd126080166bae05e26b77289	2CMV21-00163-01
7e9d8fa80e3cd36da8a466c163f40bacdac61f2d3921791b96672ed087896c9f	2CMV21-00163-01
003591a7794c5cb45904833b159cc339ef2cb8f7edfefe921b10db35ead05549	2CMV21-00165-01
01aafb8e5fa60c8d423507e4087dfb110fe78ed910294b904aee742922914450	2CMV21-00165-01
0ab7d754bdac6c7f3505368572b42ee07bc29a563bf83af2cbbc9924fc944ba9	2CMV21-00165-01
11aa9d36d7311bcd7862cbdc5eced1b698cda12fae980857732ee1ab7d5f60ac	2CMV21-00165-01
216dc98d0a9b992b98806b104dfea335abe2c28673825b0b26dda374d62b46f2	2CMV21-00165-01
374ee03189d769092fcedde30602dc310a4668b4111f96c87793c3fa6384dd6c	2CMV21-00165-01
3b6a8c70b824807b486f8d8b3d41b6810240fec4e857f427fedf8ea9cb80d8d6	2CMV21-00165-01
4ddf3a1e7b283ecc18d243c37e60b7c08d1e72a37b041b55e38ede666cc5decf	2CMV21-00165-01
66ead9fb9bfb7f17e4df8c52755e59a8eb3231d53225aff672f8d5ff859686a3	2CMV21-00165-01
725be8d9dbfdc848a9aba0826d676fc3b4daafd3169a8bb25accb2d644f91e43	2CMV21-00165-01
7a46a140079d1aa5b990531124c02994ff215004b12972b17d335bff5d4392dc	2CMV21-00165-01
7bc6d98eaa77fe1294f8c51daecb6238ecb2bd7fb62166c5c69f3ce017725731	2CMV21-00165-01
7c97c6aff3162d4a9be6ea815960d37916c37f8c02d4a84626a49d68fd089610	2CMV21-00165-01
81e5230c62a2e2a4c5cbc492eaf96fe41baa8e74e85e18462ac594518250a8d1	2CMV21-00165-01
924fc3cec5b5ba7f72c84c67f187a0ef48ef6165737e467afa23e3f6f32fae26	2CMV21-00165-01
93eae9e25fb49d513d70dc636f0bf248f5a05c6ab1662ed72660f62ab3315e33	2CMV21-00165-01
9b1dfb30b42a710d06025396d36f411a590ba357969a7fd17480e78d38bd1472	2CMV21-00165-01
9b6af086321d54ff2bd25bf1b813dc58dbaf17fb29f300d58d4eef81966f92c9	2CMV21-00165-01
9c4fe6c162057e7e0e1f8bd7cf9cbcdea59cd345af0b3cf76e9c59b09c7334d4	2CMV21-00165-01
b10f3543044812a324113b2127c205d7d135c730402126d6455bd0f79f30a5e5	2CMV21-00165-01
bacaa8f4c3663cb594f85af855915ef6d82e28fbe9eee4eff83b051d3d0a21d2	2CMV21-00165-01
c0ad412c53c697c92a3924e2532c2df0daf553e4d29175a97685e5dd2b3fe86e	2CMV21-00165-01
ca2cdc3db2d3714e1cb8aab6911cd583ccff8b5b4ec673f1152bea1ee6d0de61	2CMV21-00165-01
d6e164014a4fa3756862ec5cfe23873f4409a523f7edf38f1023c80997c3d654	2CMV21-00165-01
e0dbb2c8e0e0c6b0ae425c16db22614e680591c5fd0d8e7686294cc971ffd42d	2CMV21-00165-01
e43b4651e9d41042562b8b6f4413129f31d04f693ad7da56ee272dd4460c87f1	2CMV21-00165-01
e7334512d66ffd0a318739a73612348ceffb2bb290a915b03941764975ac9756	2CMV21-00165-01
ec4cdc6c30b24171ed2427be8b77ceab3700a362536121d840c5620b79127908	2CMV21-00165-01

f77e97a4e79b4d143ff3fb650ecc0dc2632039ccb354f0852740a7414d80306c	2CMV21-00165-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
185.222.57.232	rootlayer web services ltd.	2CMV21-00163-01
177.126.23.165	3d telecomunicacoes ltda	2CMV21-00163-01
177.185.241.139	gox internet	2CMV21-00163-01
2.136.228.191	telefonica de espana	2CMV21-00163-01
213.80.93.236	ip-only networks ab	2CMV21-00163-01
187.86.136.42	vetorialnet inf. e servicos de internet ltda	2CMV21-00163-01
99.19.124.45	att-internet4	2CMV21-00163-01
207.246.94.93	as-choopa	2CMV21-00163-01
160.16.196.187	sakura internet inc.	2CMV21-00163-01
80.82.67.51	ip volume inc	2CMV21-00163-01
185.222.57.227	rootlayer web services ltd.	2CMV21-00163-01
125.214.169.213	dialog axiata plc.	2CMV21-00163-01
195.130.35.141	University of sarajevo	2CMV21-00165-01
103.133.108.191	Vietnam posts and telecommunications group	2CMV21-00165-01
136.243.168.134	Hetzner online gmbh	2CMV21-00165-01
136.243.168.150	Hetzner online gmbh	2CMV21-00165-01
136.243.168.158	Hetzner online gmbh	2CMV21-00165-01
203.111.211.102	Savecom internation inc.	2CMV21-00165-01
103.125.191.69	Vietnam posts and telecommunications group	2CMV21-00165-01
103.99.1.148	Vietnam posts and telecommunications group	2CMV21-00165-01
104.129.30.204	Asn-quadranet-global	2CMV21-00165-01
112.78.34.85	Pt media sarana data	2CMV21-00165-01
165.22.6.20	Digitalocean-asn	2CMV21-00165-01
167.99.105.80	Digitalocean-asn	2CMV21-00165-01
172.241.27.120	Leaseweb-usa-dal-10	2CMV21-00165-01
172.93.160.149	Asn-quadranet-global	2CMV21-00165-01
185.222.58.142	Rootlayer web services ltd.	2CMV21-00165-01
186.64.118.41	Rootlayer web services ltd.	2CMV21-00165-01
200.152.67.28	Grupo tdkom	2CMV21-00165-01

211.130.170.5	Ntt communications corporation	2CMV21-00165-01
213.142.130.18	Adeoxtech	2CMV21-00165-01
45.95.169.111	Maxko j.d.o.o	2CMV21-00165-01
46.183.220.67	Dataclub s.a.	2CMV21-00165-01
68.183.193.20	Digitalocean-asn	2CMV21-00165-01

Correos electrónicos de donde son enviados los archivos adjunto con malware.

Dirección	Documento web
foodtrade@fresco.co.kr	2CMV21-00163-01
abdullaa@mashreq.com	2CMV21-00163-01
dariusz@stiens.de	2CMV21-00163-01
docusign@fstworld.com	2CMV21-00163-01
donna_perry@rogers-brown.com	2CMV21-00163-01
foodtrade3@fresco.co.kr	2CMV21-00163-01
galeman@cyrusbrokers.com.ar	2CMV21-00163-01
mariano.flores@sampa.com	2CMV21-00163-01
noreply@marklivesproducts.store	2CMV21-00163-01
ops@wmashipcare.com	2CMV21-00163-01
waruna@packserve.lk	2CMV21-00163-01
sales12@ceaworld.com	2CMV21-00163-01
statu@statushipping.com	2CMV21-00163-01
voxanhoa722@gmail.com	2CMV21-00165-01
teri@got2start.com	2CMV21-00165-01
somchai_sv@mcic.co.th	2CMV21-00165-01
sales@ohvanhorn.com	2CMV21-00165-01
sale.sg@bruker.com	2CMV21-00165-01
rosario.corpa@ctransbolivia.com	2CMV21-00165-01
reservationsgeneva@ritzcarlton.com	2CMV21-00165-01
rahul.pawar@medisponsor.com	2CMV21-00165-01
purchase_dept@rapigne-inc.com	2CMV21-00165-01
operaciones@saneamientoambientalperu.com	2CMV21-00165-01
marketing@fresco.co.kr	2CMV21-00165-01
Marcus.Abraham@Ctscp.com	2CMV21-00165-01
mahdi.saqlib@siemens.com	2CMV21-00165-01
labourecot@ecot.or.th	2CMV21-00165-01
kanya@cam-asean.com	2CMV21-00165-01
ka@flipflopbob.com	2CMV21-00165-01
info@shaheenfoundation.com	2CMV21-00165-01
info@kspnasari.co.id	2CMV21-00165-01
info@gulfogintl.com	2CMV21-00165-01
contactus@bloommaze.com	2CMV21-00165-01

Actualidad

Ministerio del Interior firma 20 nuevos convenios de ciberseguridad con entidades de todo Chile

Esta semana se llevó a cabo un nuevo encuentro entre el Ministerio del Interior y Seguridad Pública y distintas empresas y universidades, con el objetivo de realizar la firma ceremonial de 20 nuevos Convenios de Colaboración de Ciberseguridad.

La actividad, fue liderada desde el Palacio de La Moneda por el Subsecretario del Interior, Juan Francisco Galli, junto con el Jefe de División de Redes y Seguridad Informática, Carlos Landeros y la Jefa de Departamento del CSIRT de Gobierno, Katherina Canales. Mientras que de forma virtual estuvieron presentes los gerentes generales, rectores, presidentes de las 21 organizaciones partícipes: Aguas Andinas, Esval y Aguas del Valle (ambas firmaron un mismo convenio), Mutual de Seguridad, Andes Salud, Masisa, AFC, IRADE, SAAM, SB Pay, INN, Universidad de Concepción, BHP, Bolsa de Santiago, Universidad Autónoma, Essbio, Empresas Eléctricas AG, Aguas Antofagasta, Corporación de Universidades Privadas, Corporación Alta Ley y Trend Micro.

Los detalles pueden encontrarse aquí: https://www.csirt.gob.cl/noticias/csirt-firma-convenios-2021/.

Ciberconsejos para evitar caer en el phishing durante la Operación Renta

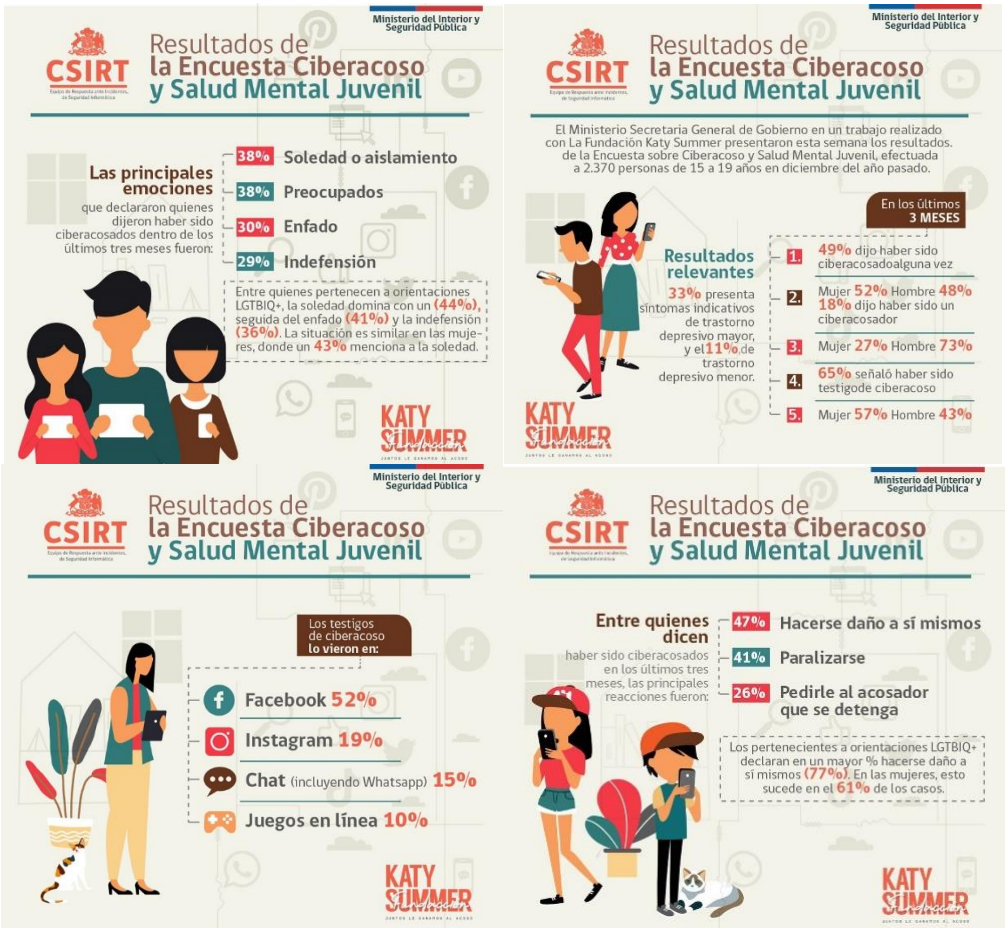
El CSIRT de Gobierno elaboró esta campaña informativa debido a que la Operación Renta genera en abril de cada año un aumento de la circulación de amenazas de ingeniería social como el phishing, riesgo que se ha visto acrecentado desde el año pasado gracias a las campañas maliciosas que se aprovechan de la pandemia y la vacunación para diseminar malware o robar datos.

Para más información, visitar aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-caer-en-el-phishing-durante-la-operacion-renta/

Estudio sobre ciberacoso y salud mental en los jóvenes | Fundación Katy Summer

La Fundación Katy Summer elaboró, junto al Ministerio Secretaría General de Gobierno, un estudio sobre salud mental y ciberacoso en adolescentes y adultos jóvenes, el que arroja preocupantes cifras de acoso virtual y tendencias depresivas en nuestro país, y refuerza la necesidad de contar con protocolos para reducir la prevalencia del ciberbullying entre nuestros jóvenes.

Más información, aquí: https://www.csirt.gob.cl/recomendaciones/estudio-sobre-ciberacoso-y-salud-mental-en-los-jovenes-fundacion-katy-summer/




Ministerio del Interior y Seguridad Pública
CSIRT
Resultados de
la Encuesta Ciberacoso
y Salud Mental Juvenil
Entre quienes dicen
haber sido ciberacosados en los últimos tres meses, las principales reacciones fueron:
14% Pide ayuda a amigos
6% Padres
1% Inspectores
Entre mujeres y miembros LGTBIQ+, afortunadamente hay una ligera mayor tendencia a pedir ayuda a amigos (17% y 19%) y padres (10% y 17%) respectivamente.
KATY SUMMER


Ministerio del Interior y Seguridad Pública
CSIRT
Resultados de
la Encuesta Ciberacoso
y Salud Mental Juvenil
En caso de ser víctima de ciberacoso
DENUNCIA
Unidad de Cibercrimen de la PDI
22708 0658
Infórmate paso a paso de como denunciar ante distintas plataformas a través de nuestra Ciberguía de Denuncia del Acoso Digital:
csirt.gob.cl/recomendaciones/ciberguia-acoso-digital
Encuentra los resultados completos en:
http://www.statknows.com/fundacionkatysummerpublico
KATY SUMMER

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 de este.

- Miguel Bastidas
- Ewald Beekman
- Ricardo Arancibia
- Camilo Iván Mix Vásquez
- Ricardo Andrés Monreal Llop
- Álvaro Salinas
- Claudio Valderrama
- Aldo Esteban Valladares Horta

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.09 15:13:46 -04'00'