Ministerio del Interior y Seguridad Pública

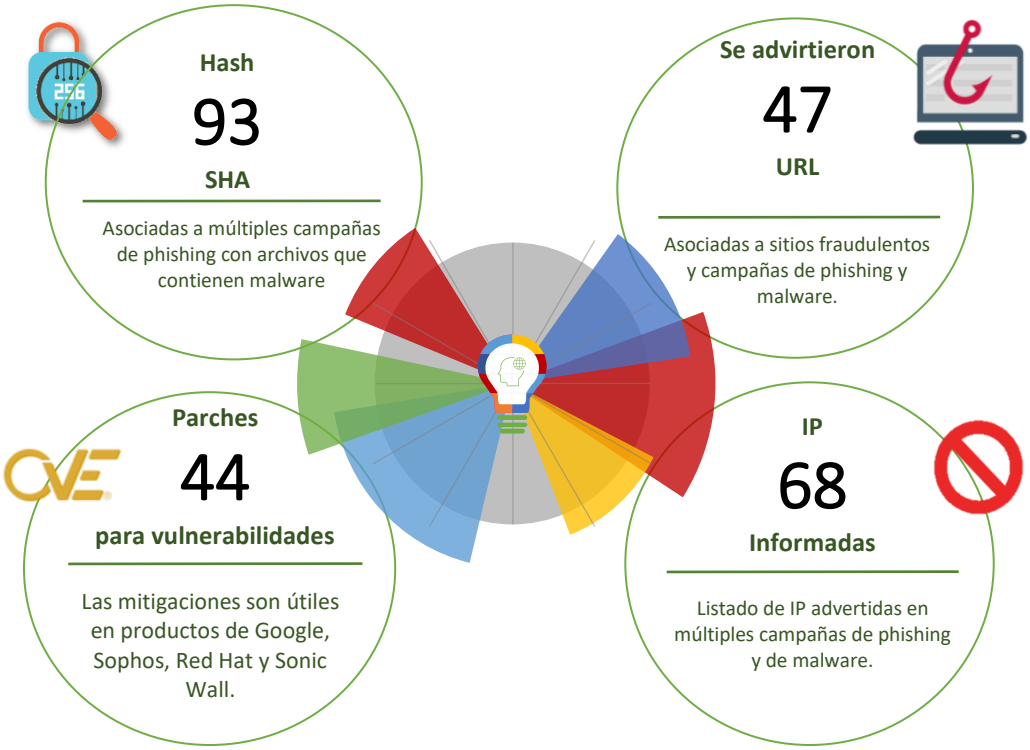
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

01-04-2022 | Año 4 | N°143

Boletín de Seguridad Cibernética

Semana del 25 al 31 de marzo de 2022

La semana en cifras



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

Contenido

Malware 2
IoC Malware 4
Phishing 12
Sitios fraudulentos 19
Vulnerabilidades 22
Actualidad 27
Muro de la Fama 30

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Malware

Imagen del mensaje

CSIRT alerta campaña de malware que suplanta a la TGR	
Alerta de seguridad cibernética	2CMV21-00289-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de marzo de 2021
Última revisión	25 de marzo de 2021
Indicadores de compromiso	
SHA256	
413ED7CDE5614D06671B4BDFD1176FE23BAB8FAD2D80367BF64A9342417FB034 859128E61625516A7357BA6A3FACE1ED8F97C580DBC889CC0FCE520DC0072346 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4 55364E85CFBF30AFA459C5D7F62DF883E94E553CAE91CB7ED2309D1F6CB455BD BB85E4530CCD6355B3EF3506548B4F513BEA844D1AF37A69624C9C455521C70F CB7F180D74DD744FE32260026CC12D051AF0C5F6E1EF31ADC387773A1B44F967 754AADC3AA19E07F2BA20217DDB0412D90E686E9965100EC7DC16475DEA2077F ABDCDAE0F174DBBA566DB5DDA98371F380C885EFB589121DB8DED98209ADD2F2 550B01B943A7C6696933CA06E3BC3A203F7FF9104BBBFA7A874E38BB65E5BC6F D666B32D2C26CDDF295433F94A637E74DB0EEDB139F4941737F2E5DAFB1D1332 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4	
IoC URL	
http://13.38.30[.]133/imbox/?/mail/u/0/#inbox/FMfcgzGmvfRcvdVbKJNggqVtCPQwxqCT https://w3tutors[.]com//sii/downlaod/#inbox/FMfcgzGmvfRcvdVbKJNggqVtCPQwxqCT https://dkloja.com[.]br/signup/file/b6c6zi5stehj19.zip	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00289-01/ https://www.csirt.gob.cl/media/2022/03/2CMV22-00289-01.pdf	

Imagen del Mensaje

CSIRT alerta ante campaña de phishing con malware que suplanta al Banco Santander	
Alerta de seguridad cibernética	2CMV21-00290-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2021
Última revisión	28 de marzo de 2021
Indicadores de compromiso	
SHA256	
C462E769265CB60487E9203F3DAC1A0AE8DEDF115EC411E56B0CBDFE5B409892 1A937ADD27C29814D1747DE6536896142D7E5360CCAABB17EB5D96C0393A21C2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0290-01/	

https://www.csirt.gob.cl/media/2022/03/2CMV22-00290-01-PH.pdf

CSIRT alerta de malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00293-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2021
Última revisión	28 de marzo de 2021
Indicadores de compromiso	
IoC URL	
http://ip-92-205-57-230.ip.secureserver[.]net/.efactura/?hash= https://swiss-services[.]com/components/com_factura/pdf/?hash= https://imunisystemrj.com[.]br/FrameworkNET8420470.zip	
SHA256	
F8B1B0322C03E7E68E433DA35260AA188140FC02A033CBD63DEA1CD8B2EDBA9C FDBF873A5B98BA84B1E2D4B32B161360E25FDAB595514666933BBB51F2F89A02 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4 F920EA86FB2B998B6499A2A2076B665BE4D034556BCB16191291D343A1B18574 754AADC3AA19E07F2BA20217DDB0412D90E686E9965100EC7DC16475DEA2077F CB7F180D74DD744FE32260026CC12D051AF0C5F6E1EF31ADC387773A1B44F967 BB85E4530CCD6355B3EF3506548B4F513BEA844D1AF37A69624C9C455521C70F 70E00AFFFD5DEA24305F669F09A5BB5BE81DE2D993CAD3AFFBFDA24BE28F7E8E 097B321EF9DA05806E6B8F94275667DA633C29C2AD618F173A7455F11D0BCB80 5C51F7DE4C41A1FCD4C42BC428A7228E29628A624BD32F2B9666D7A947078C21 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0293-01/ https://www.csirt.gob.cl/media/2022/03/2CMV22-00293-01-1.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno. Recomendamos 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	Tipo Malware	Documento web
c47af4b39af149c36ea0ae3705582699304dfd1c6d707d00bf9cfcf4f272df05	Malicious_Behavior	2CMV22-00291-01
a69a444e071dfd384f31f2744dcbd1ed1ae8e756c7bb4cab4198df70a9664179	MSIL/GenKryptik	2CMV22-00291-01
e8a002db2a2d0f8c1686efb57980906f90888da4fed1813f1eac837a7d28301c	PossibleThreat	2CMV22-00291-01
d311f1dc8ebaf910540849bc820fc160376e2c65a1a25174136c81224469c32c	HTML/Phish	2CMV22-00291-01
585a60ffb9404e720718f3c89cc96e6ee1e9052ffcc5d679c11488d4139a3d88	HTML/Phish	2CMV22-00291-01
a60903ccb76dc7d99357e356ede49aacd44e1a788282e168ff5add7227679b95	MSIL/Kryptik	2CMV22-00291-01
a8e4e5856284c881db97ff374c2e8582ab1e9df8b2ff367b44fc3675452d9c84	XF/CoinMiner	2CMV22-00291-01
2371c46ec924df7a0d316e1cf86ee518f6cd00fe56bd9e7f22b10b4413a8a2c2	W32/Injector	2CMV22-00291-01
5c5a5f5a424e0a08b69b059610d8300ba0113f149c274bac948ab16a940e8ff2	MSIL/Agent	2CMV22-00291-01
23a1abebfcdfa77ad775dfdf653651714c9958ef4b96e959869df2891b137e7a	PossibleThreat	2CMV22-00291-01
adc61c36dc1adcd24dba13ac76cb8c4477cd57558adea7b07519a23d3434116a	PossibleThreat	2CMV22-00291-01
b20a6ee4a99b06d98124806c33365c6586a3b55cabc8d1f1e0bf9a4333471040	W32/Injector	2CMV22-00291-01
d043e9ae2a1de37bf6bc144d0cadd507e6000f958acee090aea85ae9dcaedc8d	MSIL/GenKryptik	2CMV22-00291-01
e0eb50b9c44a2432107db4253c51164b94025a94949a9c0ffa55bd7a9aad98fc	MSIL/GenKryptik	2CMV22-00291-01
840729250146593d31165c8763f43475c6d58f93ad6ce25d07aec42a3cd0b38e	MSIL/GenKryptik	2CMV22-00291-01
27576b0dd2180923dfd604c136bb6500d6b7df61832ef3a57	HTML/Phish	2CMV22-00291-01

e8fe616efa1979d		
4aa607fdbdb159d41271b90aaec7e60d16ae1f255f9d237cc5258eb861dc2fe6	PossibleThreat	2CMV22-00291-01
afb419d1c3278e0e4e173f8681dbc7244fc57481e8c41a62d23ca578223ce5e2	JS/Cryxos	2CMV22-00291-01
77bd19d85d322416d7430871adb7b255079fc5ff529a5e7fe20de275ba1329ed	JS/Cryxos	2CMV22-00291-01
52be79a53489792bf445c5187e2cbd00d43ab048cc8330dee4d9cddc5a973197	MSIL/GenKryptik	2CMV22-00291-01
932751cb17ed81357dc568a2e7b9bb4b9803e4a557941c9a9516e7ca56a85e09	HTML/Phish	2CMV22-00291-01
e4d986ad03b5ae33c01512c30392d60e291a517d2b1a4d2fb26cfb502d389210	HTML/Phish	2CMV22-00291-01
942f2281a466851be7def6aa3b815ba146da4ec1da74de8f43ad3b355ea9f1d8	W32/Injector	2CMV22-00291-01
3ac0ddd1d48485ffd8dad667decd0f81e912032008e203aeb09db3ed7ba2af41	MSIL/GenKryptik	2CMV22-00292-01
2998b4c7803f7dd0b51850de9733d206a27f3c32456d0a1b8f885a752a19f830	MSIL/GenKryptik	2CMV22-00292-01
c57cc75bb01a9752a372cddbdfffcf3b5d2896d5bb6f20d12621dc479856bc3c	MSIL/GenKryptik	2CMV22-00292-01
c47af4b39af149c36ea0ae3705582699304dfd1c6d707d00bf9cfcf4f272df05	Malicious_Behavio	2CMV22-00292-01
7623a7e99590550d04cb1820e7925650a8f2b9d2879bd177aff42abb0ac80a75	MSIL/Agent	2CMV22-00292-01
040faf5a76d5b9ca793eb42251909bfe0edd54791012292ab7d63ab5f43f5fa1	MSIL/Kryptik	2CMV22-00292-01
27576b0dd2180923dfd604c136bb6500d6b7df61832ef3a57e8fe616efa1979d	HTML/Phish	2CMV22-00292-01
12dcd7587522693a443361ef3ff5dad25d87cb43646fbe5a87dfb2b7a563ab76	MSIL/Kryptik	2CMV22-00292-01
ee6536b6f9d7f13ad31c5c516828679deaf19052bf487ef52bb3ea631f0a8bfd	MSIL/GenKryptik	2CMV22-00292-01
1f3742dbfdc8062ff9716e0ee47451f9b2730b0baf42c150a6d5d56f842bdb13	MSIL/GenKryptik	2CMV22-00292-01
b0521ee5dd1378e5c88bdc7ad8f145fc6fca4ad1499aa05c1b75652c4404dfcc	MSIL/GenKryptik	2CMV22-00292-01
932751cb17ed81357dc568a2e7b9bb4b9803e4a557941c9a9516e7ca56a85e09	HTML/Phish	2CMV22-00292-01
f186b23dab51f2809732c3882e0ee1c415d1fd9e2185a94639	HTML/Phish	2CMV22-00292-01

8d65059733e0af		
7b3e7dc0b440a3248b7efcb2e8ae7f23f8b7bc19c405d9255cff42fd9a783da2	HTML/Phish	2CMV22-00292-01
34028e493361fdb64b175779438fff4297ac6f02fe883cbc2266b0352cd2a8c3	HTML/Phish	2CMV22-00292-01
8ff65bbc551448c7bdaa7d47a0a2fbce87b1d47a9b8eb1511523bb212e617696	HTML/Phish	2CMV22-00292-01
b75f765385a2deb81c8cffe896cc209d772a9bfbd5694f67174c7faec5dcc54e	MSIL/GenKryptik	2CMV22-00292-01
2437c4420b5490bb8b2bd4f041899f4863be7c59de8f0e0edb76c3d1ce6f8872	MSIL/Agent	2CMV22-00292-01
7efdf16230919315bbfb1c15e5291ba7ff5f62bc0cfe4ceb6d6aeb940a769de6	MSIL/GenKryptik	2CMV22-00292-01
bcb31780bc7bf08ffb7776f07c22f5568030c67aeb97f232aa5f3f87b5d3d834	MSIL/Kryptik	2CMV22-00292-01
1388bde6e341e2b0d7b6f4227f7de496194fd8baf006abd2c70242846390ef49	MSIL/Agent	2CMV22-00292-01
72a39125aafce6e6c68aa2c46085dc48ddec8160c87282bfd21b4e6ac7c7eb5d	MSIL/GenKryptik	2CMV22-00292-01
ccfc899656d6b39137c313ddba0f67ab3c5addcc3a2f640e36ef9f7bd5edc547	MSIL/GenKryptik	2CMV22-00292-01
0b4615b03790164f957d57c5d075dc76864baec2bd66287cff7914ef5e030b9b	W32/Injector	2CMV22-00292-01
da244395a5a963a24039e8849c6ddd4a7a341ed1567ef9e2ae9dd4805213e46f	HTML/Phish	2CMV22-00292-01
eb0054579e42b7af7bd4c037750df9f0d5e64fda4c1f3fcee92a702096e9c7e8	Malware_Generic	2CMV22-00292-01
bfb9b7a35925dacdd5d5ffdbc3bc5c7274f99d2af136df4b3fc8793d5e1540be	MSIL/GenKryptik	2CMV22-00292-01
1aef99936fc61157a354fca2ba411bfb18bdee3cccd70bd07bbfc20c586e36db	MSIL/GenKryptik	2CMV22-00292-01
8a575fc60c6cde7e8d3a25e466fdebd29e453c6f0ef40d3d441586ff15c0b112	HTML/Phish	2CMV22-00292-01
fe30cd33861d199404bfe98540c403fe1c2730924b640fb52632d7ac13cf3fa3	MSExcel/CVE_2017_11882	2CMV22-00292-01
5be44f566e19eb9e924551c4bc01d272383d26210a27962b118d6cc3dd649854	MSIL/GenKryptik	2CMV22-00292-01
af82e346bcb65fbf17289a0f5f5989dcff753c664a18572f0682a89e919f53e1	Malware_Generic	2CMV22-00292-01
def12adb6230b2df88e9e0e1c1c94720bc186cd00daa03b04	HTML/Phish	2CMV22-00292-01

12b59a515a61e1e		
8a504e1627238a6bf87622aa7bd0f38cbd78511b028be62cc3827bb5329a547a	HTML/Phish	2CMV22-00292-01
62f05a02385f5994d15b6f709dc1aeb2b144733b6c035876eeed8784e7031f72	HTML/Phish	2CMV22-00292-01
e590d3edd6eaf903220c409e152cc369cd3ee8dcbe160746ea43c3899a48817c	HTML/Phish	2CMV22-00292-01
1dca8bb8e7f598aea6a7544e68982d30d1bd6e8f3ca7ce0f3faf9a9e520bd023	HTML/Phish	2CMV22-00292-01
cbf9ddc95e1215c4346c0a588c32ed1a0da501d91eb420d354ddf2be0c413d1a	MSIL/GenKryptik	2CMV22-00292-01
b201150cd83004002dc7903f91e53868ff806757744dc11c23974029aa263b05	MSIL/GenKryptik	2CMV22-00292-01
585a60ffb9404e720718f3c89cc96e6ee1e9052ffcc5d679c11488d4139a3d88	HTML/Phish	2CMV22-00292-01
d311f1dc8ebaf910540849bc820fc160376e2c65a1a25174136c81224469c32c	HTML/Phish	2CMV22-00292-01
42b8b1208f7a193683ddcb384953140f578979d927418880f339cc1a51493309	PossibleThreat	2CMV22-00292-01
fd0156e43deb4cb9a27917ce470cf60caeee9b1eddd7f5123e51f7569717e2a7	HTML/Phish	2CMV22-00292-01
915b7231c4bfa13439dfccdf452b51de2eb77335499697896f121ad10e820bb3	HTML/Phish	2CMV22-00292-01
1d43de3fd7792a28e75cc4a863e378243855e2fcad10beb48deec869fa044304	HTML/Phish	2CMV22-00292-01
3f55a18289a4defdb2b50e5314a7972d39bd0d4e7e2da0826a91f163eebe2a9c	XF/CoinMiner	2CMV22-00292-01
df499d6e252f647ab66b0af8c7bd124e6fde172c2928612f17e6cb412f14cac1	MSIL/GenKryptik	2CMV22-00292-01

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	ASN	Documento web
157.245.11.117	DIGITALOCEAN-ASN	AS 14061	2CMV22-00291-01
190.210.196.67	NSS S.A.	AS 16814	2CMV22-00291-01

185.222.58.83	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
45.137.22.59	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
45.137.22.142	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
210.171.12.254	ITEC HANKYU HANSHIN CO.,LTD.	AS 7524	2CMV22-00291-01
185.239.243.96	AS-SERVERION	AS 399471	2CMV22-00291-01
103.207.39.102	VNPT Corp	AS 45899	2CMV22-00291-01
185.222.58.240	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
212.193.30.101	Delis LLC	AS 211252	2CMV22-00291-01
185.212.128.154	WEB_GroupInternet INC	AS 200313	2CMV22-00291-01
159.223.216.60	DIGITALOCEAN-ASN	AS 14061	2CMV22-00291-01
190.14.67.21	MegaLink	AS 22541	2CMV22-00291-01
185.222.58.58	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
65.21.100.205	Hetzner Online GmbH	AS 24940	2CMV22-00291-01
2.58.149.148	AS-SERVERION	AS 399471	2CMV22-00291-01
185.222.57.242	RootLayer Web Services Ltd.	AS 51447	2CMV22-00291-01
65.21.100.197	Hetzner Online GmbH	AS 24940	2CMV22-00291-01
185.239.243.26	AS-SERVERION	AS 399471	2CMV22-00291-01
185.222.58.83	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
185.222.57.142	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
185.222.58.240	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
157.245.11.117	DIGITALOCEAN-ASN	AS 14061	2CMV22-00292-01
138.68.42.30	DIGITALOCEAN-ASN	AS 14061	2CMV22-00292-01
209.97.129.33	DIGITALOCEAN-ASN	AS 14061	2CMV22-00292-01
65.21.100.205	Hetzner Online GmbH	AS 24940	2CMV22-00292-01
45.137.22.142	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
185.222.57.67	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
2.56.59.58	AS-SERVERION	AS 399471	2CMV22-00292-01
45.137.22.40	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
45.137.22.59	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
172.245.106.55	AS-COLOCROSSING	AS 36352	2CMV22-00292-01
194.31.98.73	Des Capital B.V.	AS 213035	2CMV22-00292-01
45.137.22.238	RootLayer Web Services Ltd	AS 51447	2CMV22-00292-01
194.31.98.105	Des Capital B.V.	AS 213035	2CMV22-00292-01
128.199.101.8	DIGITALOCEAN-ASN	AS 14061	2CMV22-00292-01

2.56.57.162	AS-SERVERION	AS 399471	2CMV22-00292-01
37.49.225.131	PEENQ.NL	AS 212370	2CMV22-00292-01
103.154.233.30	Netclues Technologies Private Limited	AS 138246	2CMV22-00292-01
144.91.103.185	Contabo GmbH	AS 51167	2CMV22-00292-01
23.94.175.131	AS-COLOCROSSING	AS 36352	2CMV22-00292-01
185.222.58.231	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01
2.58.149.148	AS-SERVERION	AS 399471	2CMV22-00292-01
103.153.77.149	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	AS 135905	2CMV22-00292-01
139.59.33.163	DIGITALOCEAN-ASN	AS 14061	2CMV22-00292-01
103.89.90.37	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	AS 135905	2CMV22-00292-01
66.96.185.7	BIZLAND-SD	AS 29873	2CMV22-00292-01
185.222.57.93	RootLayer Web Services Ltd.	AS 51447	2CMV22-00292-01

Nombres de archivo: Corresponden a aquellos documentos que vienen adjuntos en las campañas de phishing con malware. El CSIRT de Gobierno recomienda que cada institución analice las extensiones de los archivos y evalúe cuáles serán bloqueadas o permitidas. Asimismo se deben ejecutar de forma permanente las actualizaciones de los módulos de antivirus de los antispam y de las estaciones de trabajo.

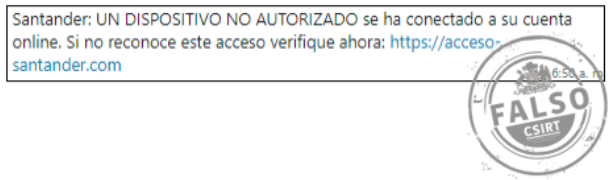
Nombre del archivo malicioso	Documento web
DEVOLUCIÃ“N DE PAGO.PDF.lzh	2CMV22-00291-01
factura 7943-5118.7z	2CMV22-00291-01
NEW ORDER.7Z	2CMV22-00291-01
Arrival Notice PSL.zip	2CMV22-00291-01
Correo_315.xls	2CMV22-00291-01
tk8494.cab	2CMV22-00291-01
PACIFIC PDA TEMPLATE FOR MV GULF WIND.img	2CMV22-00291-01
00009453725262.GZ	2CMV22-00291-01
winmail.dat.exe	2CMV22-00291-01
INVOICE.pdf.7z	2CMV22-00291-01
TNT Original Invoice.zip	2CMV22-00291-01
PAGO 422062218.rar	2CMV22-00291-01

OVER DUE INVOICES_12-08-2021.pdf.bat.gz	2CMV22-00291-01
FINAL DEMAND_REF-ATA173899.html	2CMV22-00291-01
BANK DETAILS CONFIRMATION.zip	2CMV22-00291-01
PO#3260913.PDF.html	2CMV22-00291-01
AB-Q20222903.zip	2CMV22-00291-01
Quotation 104469.html	2CMV22-00291-01
Z220BTYUII32457897.ace	2CMV22-00291-01
Quotation.GZ	2CMV22-00292-01
HBL draft Copy.LZH	2CMV22-00292-01
Revised Proforma Invoice.BZ2	2CMV22-00292-01
DEVOLUCIÃ“N DE PAGO.PDF.lzh	2CMV22-00292-01
lista de pedidos y productos solicitados.img	2CMV22-00292-01
Scan USD71,450, 13774477859448857747676574888383737327277722 pdf.rar	2CMV22-00292-01
FINAL DEMAND_REF-ATA173899.html	2CMV22-00292-01
Reminder quotation.zip	2CMV22-00292-01
Payment advice.rar	2CMV22-00292-01
Aldora proforma invoice (2).zip	2CMV22-00292-01
PL.lzh	2CMV22-00292-01
AWB Shipping Invoice.html	2CMV22-00292-01
Paid Invoice.shtml	2CMV22-00292-01
update-process.html	2CMV22-00292-01
Order 4566789.r09	2CMV22-00292-01
ENQ5067600003.img	2CMV22-00292-01
Scan USD71,450, 13774477859448857747676574888383737327277722 pdf.exe.zip	2CMV22-00292-01
DHL-AWB.gz	2CMV22-00292-01
PO.img	2CMV22-00292-01
New Purchase Order 4790975157.pdf.rar	2CMV22-00292-01
Slip76875987.rar	2CMV22-00292-01
Lista de ordenes de compra.zip	2CMV22-00292-01
Revised Contract.xlsx	2CMV22-00292-01
Quotation 005538.z	2CMV22-00292-01
Payment Processed.zip	2CMV22-00292-01
Invoice.doc	2CMV22-00292-01

PO#3260913.pdf.gz	2CMV22-00292-01
REQUEST FOR QUOTATION OUR REF TRENT-2587.xlsx	2CMV22-00292-01
Maersk BL 216238068.zip	2CMV22-00292-01
AWB_006647837575.pdf.r01	2CMV22-00292-01
SOA SCAN COPY.UUE	2CMV22-00292-01
FILE-03302022.xls	2CMV22-00292-01
PO.zip	2CMV22-00292-01

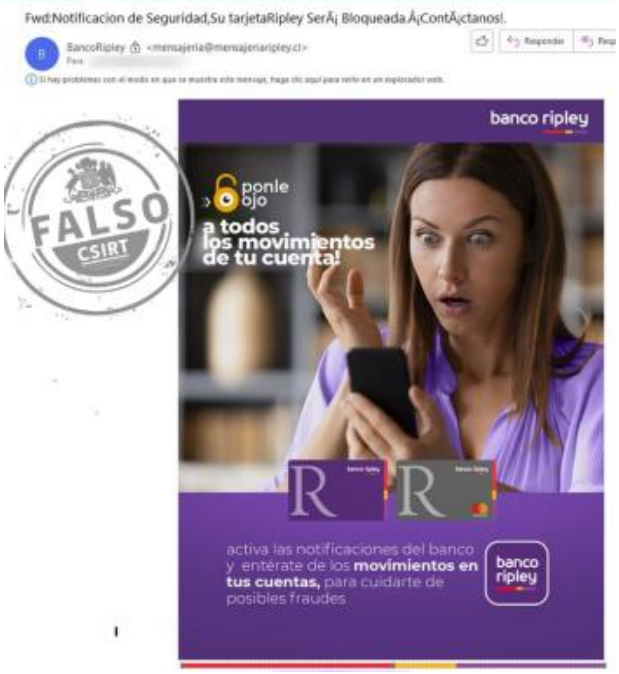
Phishing

Imagen del mensaje



CSIRT advierte phishing por dispositivo no autorizado suplantando al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00490-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de marzo de 2022
Última revisión	25 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://acceso-santander[.]com/control.php	
IP	
[2.56.59.181]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00490-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00490-01.pdf	

Imagen del mensaje



CSIRT informa sobre phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00491-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de marzo de 2022
Última revisión	25 de marzo de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3Jz7Mvi?l=www.bancoripley.cl http://xn--119-hy7mx2m78r[.]kr/assets/bootstrap/css/enviar03.php?l=629711948 https://bit[.]ly/3umlsn1?l=www.bancoripley.cl https://wardatalwadirealestates[.]com/activacion/cuenta-chrr/	
URL sitio falso	
http://bancoripley-cl.tracysuccess[.]com/1648214488/login	
IP	
[111.235.137.123]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00491-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00491-01.pdf	

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Imagen del mensaje

CSIRT advierte phishing con falsos puntos suplantando al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00492-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://santanderpunto.org/control.php	
IP	
[2.56.59.181]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00492-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00492-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por dispositivo no autorizado suplantando al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00493-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL redirección	
https://catimex.com[.]mx/wp-content/languages/–/Bloqueio_Tarjeta/	
URL sitio falso	
https://email-tarjeta[.]com/control.php	
IP	
[2.56.59.181]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00493-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00493-01.pdf	

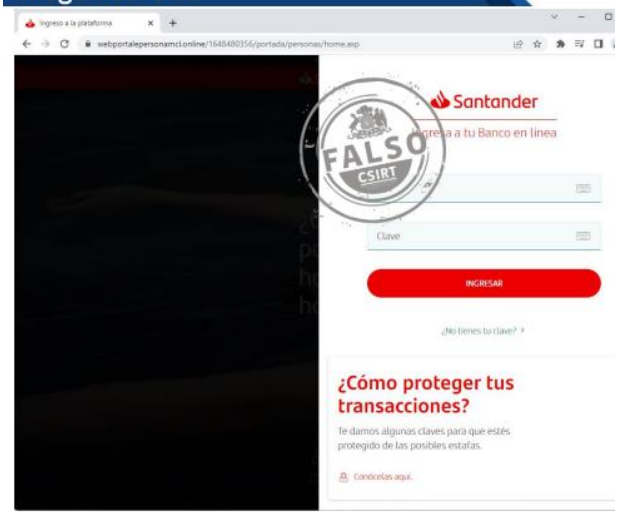
Imagen del mensaje

CSIRT alerta phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00494-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://laurus.ph/	
IP	
[216.218.206.35]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00494-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00494-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00495-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://www-bancoripley-cl.musicchains[.]net/1648475615/login	
URL redirección	
https://bit.ly/3iyHIo8?l=www.bancoripley.cl http://xn--119-hy7mx2m78r.kr/assets/bootstrap/css/enviar.php https://bit.ly/3umlsn1?l=www.bancoripley.cl https://wardatalwadirealestates[.]com/activacion/cuenta-chrr/	
IP	
[104.219.250.6]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00495-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00495-01.pdf	

Imagen del sitio



CSIRT informa phishing vía WhatsApp que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00496-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://webportalepersonamcl[.]online/1648479981/portada/personas/home.asp	
URL redirección	
http://ow.ly/Q1rn50IsVQ8	
IP	
[104.219.250.6]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00496-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00496-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing por WhatsApp que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00497-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de marzo de 2022
Última revisión	28 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
http://hk54.hkwordpress[.]com/poque	
URL redirección	
https://contriplay.net/ganador/cuenta-scgi/	
IP	
[143.95.225.99]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00497-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00497-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00498-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.itaupuntos[.]digital/726a292db52f7f5/html/index.php	
URL redirección	
http://ec2-34-238-41-18.compute-1.amazonaws[.]com/D0190238787912-3/?hash=bnVsbEBudWxsLmNs	
IP	
[3.86.149.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00498-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00498-01.pdf	

Imagen del mensaje

CSIRT informa phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00499-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://www-bancoripley.cl.spinlinen.co[.]za/1648728662/login	
URL redirección	
https://bit[.]ly/3Dou4O0?l=www.bancoripley.cl http://xn--119-hy7mx2m78r[.]kr/assets/bootstrap/css/enviar02.php?l=1540667815 https://bit[.]ly/3umPxD8?l=www.bancoripley.cl https://wardatalwadirealestates[.]com/activacion/cuenta-hiia/	
IP	
[5.134.8.84]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00499-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00499-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing con falso aumento de cupo de la tarjeta	
Alerta de seguridad cibernética	8FPH22-00500-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://personas-chile[.]cf/1648732150/bchile-web/persona/login/index.html/login	
URL redirección	
https://bit[.]ly/portal_consumo https://parasolbook[.]com/chile.php https://xcl-persona[.]nl/	
IP	
[91.209.70.109]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00500-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00500-01.pdf	

Imagen del mensaje

CSIRT advierte phishing usurpando la identidad del BancoEstado	
Alerta de seguridad cibernética	8FPH22-00501-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://katka-masopustova[.]cz/mnkghy/pagina/imagenes/comun2008/banca-en-linea_personas.html	
URL redirección	
https://contriplay.net/ganador/cuenta-scgi/	
IP	
[81.95.96.90]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00501-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00501-01.pdf	

Imagen del mensaje

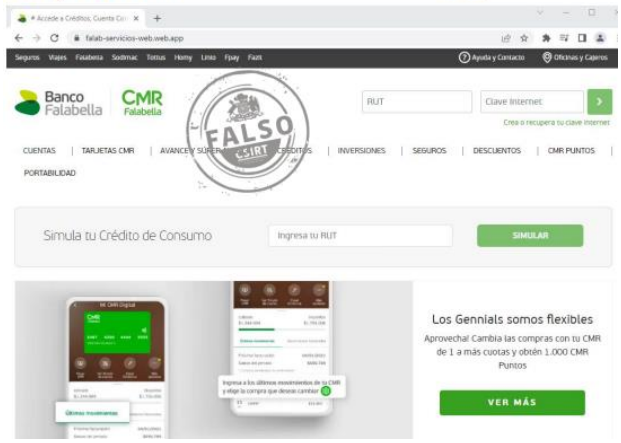
CSIRT advierte phishing con falso bloqueo de tarjeta	
Alerta de seguridad cibernética	8FPH22-00502-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
http://uthh.edu[.]mx/content/public/Support/pagina/imagenes/comun2008/banca-en-linea-personas.html	
URL redirección	
https://nscf.co[.]za/content/bancoestado-public/home/	
IP	
[187.191.80.132]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00502-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00502-01.pdf	

Imagen del mensaje

CSIRT advierte phishing con falsos puntos del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00503-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://itautarjeta[.]online/726a292db52f7f5/html/index.php	
URL redirección	
http://ec2-34-238-41-18.compute-1.amazonaws[.]com/D0190238787912-3/?hash=bnVsbEBudWxsLmNs	
IP	
[3.86.149.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00503-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00503-01.pdf	

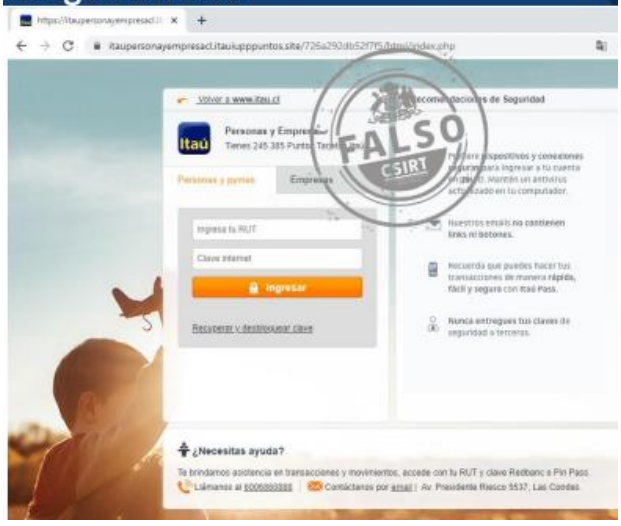
Sitios fraudulentos

Imagen del sitio



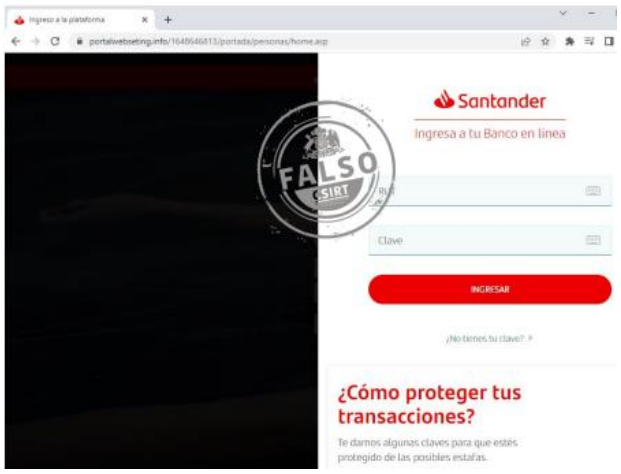
CSIRT advierte sitio falso del Banco Falabella	
Alerta de seguridad cibernética	8FFR22-01067-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://falab-servicios-web.web[.]app/	
IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01067-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01067-01.pdf	

Imagen del sitio



CSIRT informa suplantación del sitio web del Banco Itaú	
Alerta de seguridad cibernética	8FFR22-01068-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://itaupersonayempresacl.itauiupppuntos[.]site/726a292db52f7f5/html/index.php	
IP	
[3.86.149.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01068-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01068-01.pdf	

Imagen del sitio

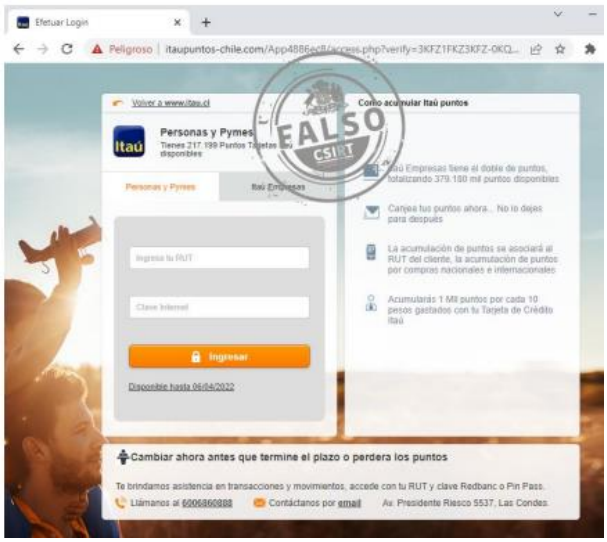


CSIRT advierte página web falsa del Banco Santander	
Alerta de seguridad cibernética	8FFR22-01069-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://portalwebseting[.]info/1648646813/portada/personas/home.asp	
IP	
[162.241.62.4]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01069-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01069-01.pdf	

Imagen del sitio

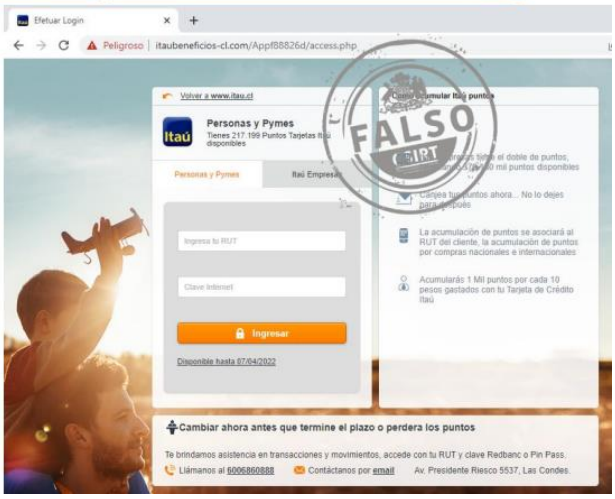
CSIRT informa página web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01070-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://www-santander.p3rsonas[.]net/	
IP	
[108.174.196.214]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01070-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01070-01.pdf	

Imagen del sitio



CSIRT advierte suplantación del sitio web del Banco Itaú	
Alerta de seguridad cibernética	8FFR22-01071-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://itaupuntos-chile[.]com/	
IP	
[20.226.60.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01071-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01071-01.pdf	

Imagen del sitio



CSIRT informa página web que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR22-01072-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://itaubeneficios-cl[.]com/Appf88826d/access.php	
IP	
[20.226.60.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01072-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01072-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en Google Chrome y navegadores derivados	
Alerta de seguridad cibernética	9VSA22-00600-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de marzo de 2022
Última revisión	29 de marzo de 2022
CVE	
CVE-2022-1096	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones anteriores a la 99.0.4844.84. Microsoft Edge, versiones anteriores a la 99.0.1150.55. Opera Vivaldi Chromium	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00600-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00600-01.pdf	

CSIRT alerta ante vulnerabilidad crítica en Sophos Firewall	
Alerta de seguridad cibernética	9VSA22-00601-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de marzo de 2022
Última revisión	14 de marzo de 2022
CVE	
CVE-2022-1040	
Fabricante	
Sophos	
Productos afectados	
Sophos Firewall de 17.0.0 a 18.5.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00601-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00601-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en productos Red Hat		
Alerta de seguridad cibernética	9VSA22-00602-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	29 de marzo de 2022	
Última revisión	29 de marzo de 2022	
CVE		
CVE-2021-0920	CVE-2022-22826	CVE-2022-25236
CVE-2021-4083	CVE-2022-25235	CVE-2022-22824
CVE-2022-0330	CVE-2022-23852	CVE-2022-25315
CVE-2022-22942	CVE-2021-46143	CVE-2022-25235
CVE-2022-25315	CVE-2022-22827	CVE-2022-25236
CVE-2021-45960	CVE-2022-22822	CVE-2022-22720
CVE-2022-22825	CVE-2022-22823	CVE-2022-0778
Fabricante		
Red Hat		
Productos afectados		
Red Hat Enterprise Linux Server – AUS 7.6 x86_64 Red Hat Enterprise Linux Server – TUS 7.6 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions 7.6 ppc64le Red Hat Enterprise Linux Server – Update Services for SAP Solutions 7.6 x86_64 Red Hat Enterprise Linux for Power, little endian: 7 Red Hat Enterprise Linux for Power, big endian: 7 Red Hat Enterprise Linux for IBM z Systems: 7 Red Hat Enterprise Linux for Scientific Computing: 7 Red Hat Enterprise Linux Desktop: 7 Red Hat Enterprise Linux Workstation: 7 Red Hat Enterprise Linux Server: 7 expat (Red Hat package): anteriores a 2.1.0-14.el7_9 Red Hat Enterprise Linux Server – TUS: 8.2 expat (Red Hat package): anteriores a 2.2.5-3.el8_2.2 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le		

openssl (Red Hat package): 1.1.1k-5.el8_5
Red Hat Enterprise Linux for ARM 64: 8
Red Hat Enterprise Linux for Power, little endian: 8
Red Hat Enterprise Linux for IBM z Systems: 8
Red Hat Enterprise Linux for x86_64: 8.0
Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server – TUS: 8.4
Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.4
Red Hat Enterprise Linux Server – AUS: 8.4
openssl (Red Hat package): anterior a 1.1.1g-16.el8_4
openssl (Red Hat package): 1.0.2k-9.el7_4
Red Hat Enterprise Linux Server – AUS: 7.4
Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 7.7
Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 7.7
Red Hat Enterprise Linux Server – TUS: 7.7
Red Hat Enterprise Linux Server – AUS: 7.7
openssl (Red Hat package): before 1.0.2k-21.el7_7
openssl (Red Hat package): 1.0.1e-61.el7_3
Red Hat Enterprise Linux Server – AUS: 7.3
Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.4
Red Hat Enterprise Linux Server – TUS: 8.4
Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.4
Red Hat Enterprise Linux for IBM z Systems – Extended Update Support: 8.4
Red Hat Enterprise Linux Server – AUS: 8.4
Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.4
Red Hat Enterprise Linux for ARM 64 – Extended Update Support: 8.4
Red Hat Software Collections: 1 for RHEL 7
Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server – AUS 7.7 x86_64
Red Hat Enterprise Linux Server – TUS 7.7 x86_64
Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions 7.7 ppc64le
Red Hat Enterprise Linux Server – Update Services for SAP Solutions 7.7 x86_64

Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00602-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00602-01.pdf

CSIRT alerta ante vulnerabilidad crítica de SonicWall	
Alerta de seguridad cibernética	9VSA22-00603-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2022
Última revisión	30 de marzo de 2022
CVE	
CVE-2022-22274	
Fabricante	
Sonic Wall	
Productos afectados	
TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870: versión 7.0.1-5050 y anteriores. NSsp 15700: versión 7.0.1-R579 y anteriores. NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600: versión 6.5.4.4-44v-21-1452 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00603-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00603-01.pdf	

CSIRT informa sobre vulnerabilidades parchadas en Google Chrome 100		
Alerta de seguridad cibernética	9VSA22-00604-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	15 de marzo de 2022	
Última revisión	15 de marzo de 2022	
CVE		
CVE-2022-1125	CVE-2022-1133	CVE-2022-1141
CVE-2022-1127	CVE-2022-1134	CVE-2022-1142
CVE-2022-1128	CVE-2022-1135	CVE-2022-1143
CVE-2022-1129	CVE-2022-1136	CVE-2022-1144
CVE-2022-1130	CVE-2022-1137	CVE-2022-1145
CVE-2022-1131	CVE-2022-1138	CVE-2022-1146
CVE-2022-1132	CVE-2022-1139	
Fabricante		
Google		

Productos afectados
Google Chrome anteriores a Chrome 100.0.4896.60.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00604-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00604-01.pdf

Actualidad

Ciberguía | Estafas y malware relacionados con las criptomonedas

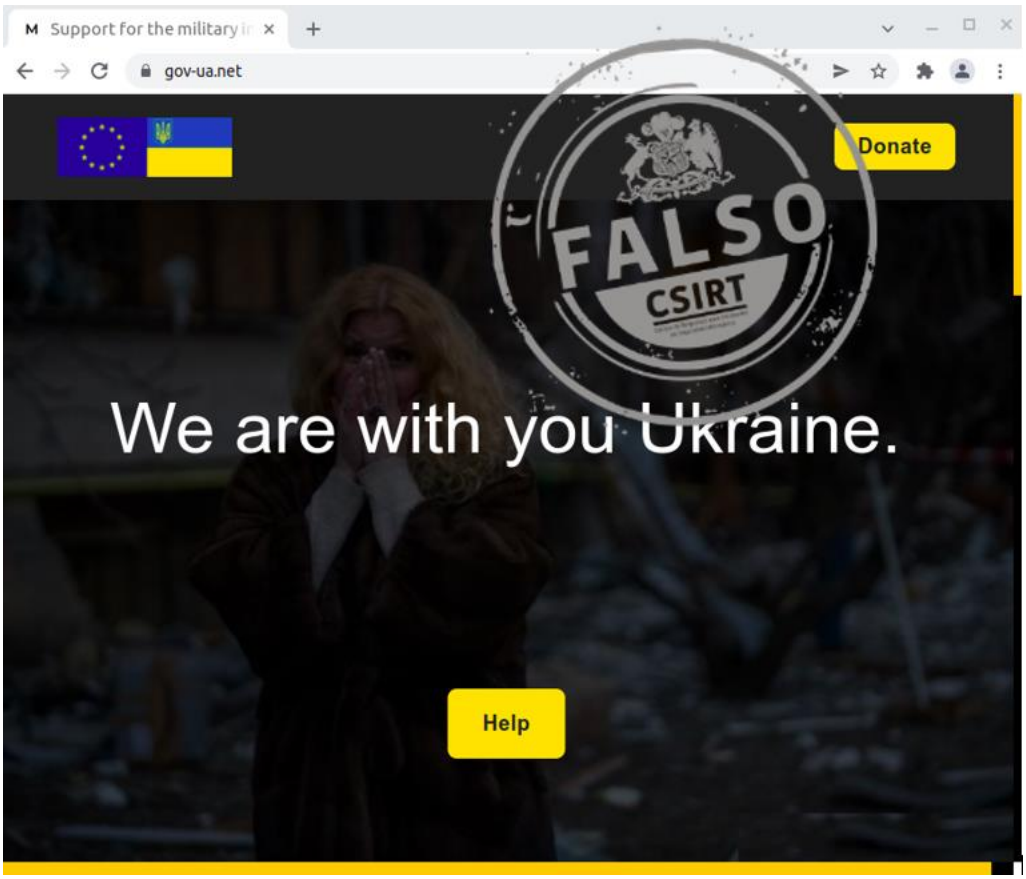
Con el creciente interés en las denominadas criptomonedas, también han aumentado los fraudes que se apoyan en ellas. Por esto les traemos una serie de recomendaciones para evitar ser víctima de estafas con criptomonedas y criptoactivos, o que nos convirtamos en involuntarios "mineros" para los ciberdelincuentes.

Conoce las estafas más comunes con criptomonedas, descargando nuestra guía aquí: https://www.csirt.gob.cl/recomendaciones/ciberguia-estafas-y-malware-relacionados-con-las-criptomonedas/.

Ciberdelincuentes realizan estafas con falsa ayuda a Ucrania

A pesar del drama que significa la actual guerra de agresión impuesta por Rusia sobre Ucrania, los estafadores virtuales se aprovechan del gran interés que ha generado la posibilidad de realizar digitalmente donaciones en dinero con la finalidad de apoyar a Ucrania para, con páginas web falsas, correos electrónicos y campañas a nivel mundial a través de redes sociales, quedarse con el dinero de las personas.

Para tener más información sobre este tipo de estafas y enlaces para aportar a Ucrania con seguridad, visiten nuestro sitio: https://www.csirt.gob.cl/noticias/falsa-ayuda-ucrania/



https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

Recomendaciones y buenas prácticas

- 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.

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

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 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 (csirt.gob.cl o al 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Georgina Patricia Escalona Fuenzalida
- Juan Alfonso Muñoz Castañeda
- Víctor Hugo González Soto
- Patricio Vergara Martínez
- Simón Herrera
- Sebastián M.
- Bárbara Palacios Cabezas
- Yasmín Salinas
- Jair Palma
- Rocío Loreto Jorquera Santander
- Karla Aravena Quiroz
- Ernesto Alonso Riquelme Arroyo
- Carlos Humberto de la Fuente Castro
- Beatriz Pérez
- Tomás Gaete
- Cristián Pérez Villarroel