Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

11-1-2022 | Año 4 | N°175

Boletín de Seguridad Cibernética

Semana del 04 al 11 de noviembre de 2022

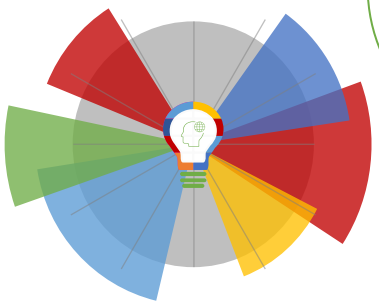
La semana en cifras

Parches

81

para vulnerabilidades

Las mitigaciones son útiles en productos de VMware, Microsoft, y Cisco.



IP

10

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

Se advirtieron

17

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

65

Asociadas a múltiples campañas de phishing con archivos que contienen 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 de campaña de phishing con malware Emotet	
Alerta de seguridad cibernética	2CMV22-00373-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de noviembre de 2022
Última revisión	4 de noviembre de 2022

Indicadores de compromiso

Asunto

Fwd:Margarita Estefanía Muñoz Bustamant MIME-Version: 1.0

Correo de Salida

o.ahmed@texitech.com

SHA256

1ef2d28fecc89437e72d6a1c1b062b5448d8d433493ca35776c1a409e436bf70
7e8bc31fde2acc45f23d277c2e9ea931aec4bb3048571ee1244856b3b8607f48
9552854e3bd6e3564eb8721075c7c4f173cb8aac03f81ca00bda024792df7456
d782617037404b290565214464f9bb696021c8417330b603d777dd78d4d69caf
58483f9342bc43f1e90455b20f8964aa00b36cfec4600731357932b64f02fabd
bfcbc9960fc804ae556e210bbb59931156d71a0ec731101bca1d5d96f9f09338

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-00373-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00373-01.pdf

Imagen del mensaje

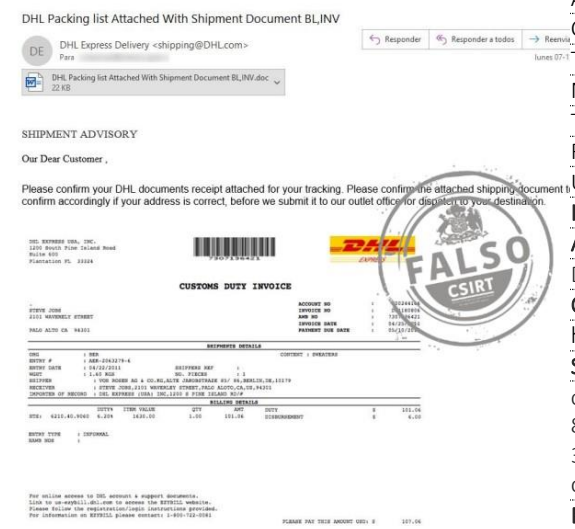
CSIRT comparte información de nueva campaña de phishing con malware Emotet	
Alerta de seguridad cibernética	2CMV22-00375-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
Re: PROPIR INICIAL 2020 REGION DE MAGALLADE LA ANTÁRTICA CHILENA	
Correo de Salida	
martin@electrodiesel.co.za	
SHA256	
893798c86bda1e6bca3af93c4dcfacd87ffe7ead8241afc28fe781a96f014ecf 4a2cb00e3782efb6826b6e5560f7b5d088dd0700e9f222df49da1331c98396ed	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00375-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00375-01.pdf	

Imagen del mensaje

CSIRT alerta de nueva campaña de phishing con malware Emotet	
Alerta de seguridad cibernética	2CMV22-00376-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
Catalina Mulet Díaz	
Correo de Salida	
antonio.mena@casamazatlan.mx	
SHA256	
4a95813a931573eda14872be0e9197063dd86cda1e204ec48ebdf11bcaa3c382 b9eee623a848474899bf25709dc654346c764143d45038ef055220da70119f0f 1b53df69b2636b83de568a7c552fd1f08050048a88d97dcb7d5fe4bfc0c23a6e a43722e040c9e3abbe54902f4a298dde6fc4e4b81afc244205ad2fa47b6df7b8	
Enlaces para revisar el informe:	

https://www.csirt.gob.cl/alertas/2cmv22-00376-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00376-01.pdf

Imagen del mensaje



CSIRT alerta de campaña de phishing con malware, que suplanta a DHL	
Alerta de seguridad cibernética	2CMV22-00377-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
DHL Packing list Attached With Shipment Document BL,INV	
Correo de Salida	
hp0.wx16.mxox.live	
SHA256	
c1cd4a1045851e4f1abd489ca80fe24188079a20d92b0151e98c4de7e18086e2 3fea3f6495a47986f614e1c2f360b959b3a0bd49bba695b7e06eeb6500fdd6cf	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00377-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00377-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing con malware en falsa factura	
Alerta de seguridad cibernética	2CMV22-00378-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
Reciba su Factura digital Factura digital	
Correo de Salida	
blog@server2.inoneapp.in facturaenlinea@network.org nouth@hermes.saludbcs.gob.mx postmaster@maildc1526907199.mihandns.com test@takaraume.com ftp@075-128-162-229.biz.spectrum.com nouth@nordis.services nouth@krw0.media247.org	

postgres@email.schp.cz postmaster@vmi1002928.contaboserver.net contato@plenitudegnm.com jessica@dedodegente.com.br vendasg5@alljeep.com.br nouth@csh0.elitex3.org nouth@crk0.elitek2.org nouth@us1.thancloud.com nouth@nordis.ltd nouth@nordiss.co.in nouth@nordiss.info nouth@nordiss.live nouth@nordis.today nouth@nordiss.club postmaster@syd-01.timetink.com.au nouth@nordis.life nouth@mta7.nordis.life nouth@mta2.nordis.life nouth@nordis.agency web@hirodenkoso.or.jp alfonso.sanchez@bralo.com.mx nouth@tradetnz.info nouth@ip41.ip-15-204-42.us
SHA256
bed758b329ea2a32d2e5bfa652848a45338b4483f7ab882517ce8c008b39e292 31416f0eee87c91027ddedffdf9010b397d3880d3504575d48abbefbb8696bf4 b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4 bb2621a454221295f04328f74dc5b5e98a6218a60db3fc488ffe0c78726a9957 5236b005d49d9b6d220b33a365c134f6cba8363829432d5b144d952418f37536 237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00378-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00378-01.pdf

Imagen del mensaje

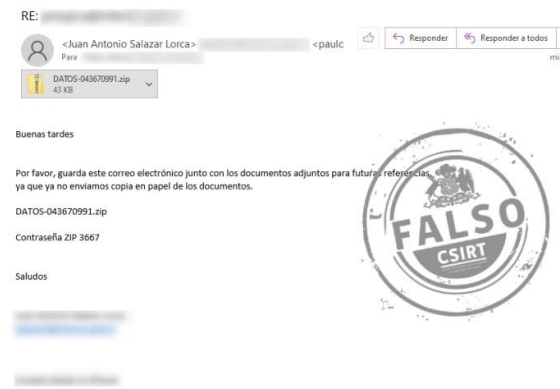
CSIRT alerta de campaña de phishing con malware en falsa cotización	
Alerta de seguridad cibernética	2CMV22-00379-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
COTIZACION ARTICULOS DE OFICINA PARA PRODUCCION	
Correo de Salida	
yazmin.sepulveda@alsea.com.mx	
SHA256	
141db01f957472533d9791c5fb883b442d25d557497c0b6b94961fb64330a57f 2a93ae1bd54ea0587fac5a180e8f098cb5e5db2ff877ce5d8c82e1db1844c4fd	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00379-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00379-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing con malware, que suplanta a Recoleta	
Alerta de seguridad cibernética	2CMV22-00380-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
Asunto	
RE:	
Correo de Salida	
alefi@laredologistica.com.br	
SHA256	
31b5df865e37e0984f064397bafac9579ad2a50467318e2949d258148fb1e59e 1be10e9a4e3ddb2ba28a3d1951a96ce11c65669edcee13fa937d3fbbedf21a01 6a22b6a0b19dc7a5650f30e47e99380bc5bad683725e8a73622221122bf0b31d 968e02fbdf7a92c4f831564742c326960c1e25d70c71028f98852c83e808fb4d cec081687f476a1310f4afe8e37ebf5db1f0e720c3f8110157679c242e0e3f31	

Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00380-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00380-01.pdf

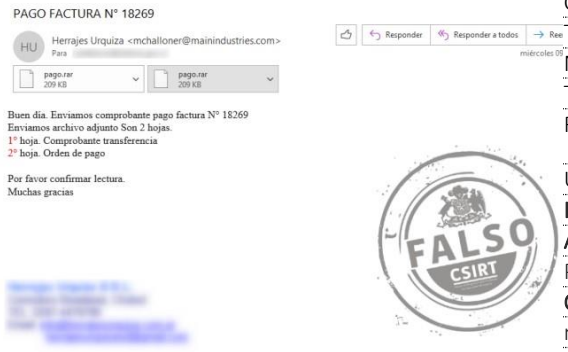
Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta a Recoleta	
Alerta de seguridad cibernética	2CMV22-00381-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022

Indicadores de compromiso
Asunto
RE:
Correo de Salida
paulo.sergio@aquilaexpress.com.br
SHA256
33beb4235033cc961396d4f5e09b06d7fc980e373dd47123d2efe266a2b8ec65 2b704ae029e158e78a33489dfe8c3b8c843bfc3b9d248d54e58faebb9971d004 6157e20809d809be949b809c806dd933d4a4a34b3fae01db5e09c3dea3916b17 f7972e53d6a16c688cf26019209b36ca02e37cd0baf9c918c79fe55fa51a5ac6 39e0063d406edc05ac8d8c1ac8a16ee63b154fa52be59fc8f07458809fb218b7
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00381-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00381-01.pdf

Imagen del mensaje



CSIRT alerta ante campaña de phishing con malware en falsa factura	
Alerta de seguridad cibernética	2CMV22-00382-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
Indicadores de compromiso	
Asunto	
PAGO FACTURA N° 18269	
Correo de Salida	
mchalloner@mainindustries.com	
SHA256	
a2a9037df8103a210d796e93ae6036969ced937688584a0de9027592495da977 d82eb8895f598f8eae3c303e4b4aa200acf783b5a75baeb789a64539589468e2 6dcfedd572210432348da3f3632e222821fcfc7bd3a91d25d7505649afe23ea9 90c14e72805950724bbd1f342261c16d88fd1e53e292c515fd135034057204b3 7e62912c1b3c994abb1503fb3034f6c8b97504286a797b066363bbda86288040	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00382-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00382-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing con malware Emotet en falso documento	
Alerta de seguridad cibernética	2CMV22-00383-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
Asunto	
RE:	
Correo de Salida	
gerencia@neoortopedia.com	
SHA256	
a2a9037df8103a210d796e93ae6036969ced937688584a0de9027592495da977	

d82eb8895f598f8eae3c303e4b4aa200acf783b5a75baeb789a64539589468e2 6dcfedd572210432348da3f3632e222821fcfc7bd3a91d25d7505649afe23ea9 90c14e72805950724bbd1f342261c16d88fd1e53e292c515fd135034057204b3 7e62912c1b3c994abb1503fb3034f6c8b97504286a797b066363bbda86288040
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00383-01/
https://www.csirt.gob.cl/media/2022/11/2CMV22-00383-01.pdf

Imagen del mensaje

CSIRT alerta por campaña de phishing con malware, que suplanta a la Municipalidad de Requínoa	
Alerta de seguridad cibernética	2CMV22-00384-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
Asunto	
RE:	
Correo de Salida	
giulianna@federaltraducoes.com.br	
SHA256	
9283a997447b09f5c50f5c189eb66cf687065514181f22511fc80454d28c7784 7d34bfd86fba89924215e960a2a68ca3de2e2ccdfb2a6e418517566dde151c15 78b7f834255ee4c7e897393c70172de692415c784bcaeedf1cd304fe1ce401e0 4706e64a038f48eea70b17e8f597ed97c518ae07c20ade6f699f1149d608e77d 7c5c7f2f5d661e47be60eaae824e2ae18e43e76e0dfa5006571cf74266677cd7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00384-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00384-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de phishing con malware, que suplanta a Emasa	
Alerta de seguridad cibernética	2CMV22-00385-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de noviembre de 2022
Última revisión	10 de noviembre de 2022
Indicadores de compromiso	
Asunto	
RE: FACTURA ADJUNTA CON SWIFT DE PAGO (MT103)	
Correo de Salida	
ecommerce@emasa.cl	
SHA256	
8d97cb1af2d4f226c632ba19bdb4275a6bcd7bde14331acdf6e05512634e385f 287f7ae3c0e5f551e6f6404b2865f562e532e766e1d8726ba6cbb62ded053d1b 11ae277dfa39e7038b782ca6557339e7fe88533fe83705c356a1500a1402d527 ab6cac56777db33f1066f42ade1006a046b5e53bc330dfd6c71301da385cc6c7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00385-01/	
https://www.csirt.gob.cl/media/2022/11/2CMV22-00385-01.pdf	

Sitios fraudulentos

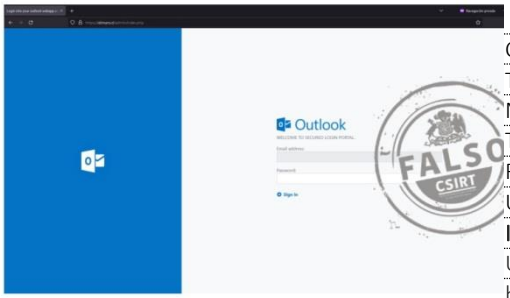
Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01131-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://santanderchile-personas.xliterestaurant[.]com/1667770065/portada/personas/home.asp	
IP	
[45.40.134.229]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01131-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01131-01.pdf	

Imagen del sitio

CSIRT alerta sitio fraudulento que suplanta a Santa Isabel	
Alerta de seguridad cibernética	8FFR22-01132-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://divisionstagnate.cn/SantaIsabelws/tb.php?ea=be1667828746300	
https://8yue22.cn/0W6Y2ZOX/SantaIsabelws/?_t=1667910410841#1667910416599	
IP	
[104.21.77.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01132-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01132-01.pdf	

Imagen del sitio



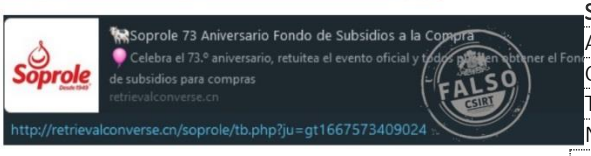
CSIRT alerta de página fraudulenta que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR22-01133-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://idimaro.cl/admin/index.php	
IP	
[200.73.115.31]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01133-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01133-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR22-01134-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
hxxps://mard[.]cl/Users/apps/netflix/backuppagenetfix/zd/clients	
IP	
[190.107.176.120]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01134-01/	
https://www.csirt.gob.cl/media/2022/11/8FFR22-01134-01.pdf	

Phishing

Imagen del mensaje



CSIRT alerta campaña de phishing por WhatsApp que suplanta a Soprole	
Alerta de seguridad cibernética	8FPH22-00634-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de noviembre de 2022
Última revisión	5 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://retrievalconverse.cn/soprole/tb.php?ju=gt1667573409024	
https://upceshop.cn/o4hfodFS/soprole/?_t=1667671047609#1667671050703	
IP	
[172.67.182.117]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00634-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00634-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta login de email	
Alerta de seguridad cibernética	8FPH22-00635-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bafybeifdyyowrw4p6e5sf52krlvnk7xjrjwhf5qioxoweutgmzcfsmgvym.ipfs.w3s[.]link/azgwo_cham-e263868.html#test@csirt.gov.cl	
URL sitio falso	
https://bafybeifdyyowrw4p6e5sf52krlvnk7xjrjwhf5qioxoweutgmzcfsmgvym.ipfs.w3s[.]link/azgwo_cham-e263868.html#test@csirt.gov.cl	
IP	
[172.64.146.135]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00635-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00635-01.pdf	

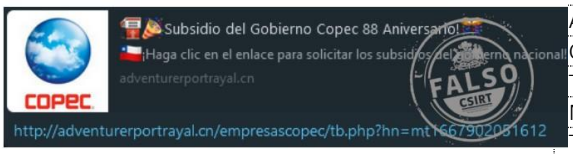
Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00636-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de noviembre de 2022
Última revisión	7 de noviembre de 2022
Indicadores de compromiso	
7 de noviembre de 2022	
https://nostracontrical[.]com/promociones/cuenta-avhh/	
URL sitio falso	
https://personaview[.]top/1667852374/portada/personas/home.asp	
IP	
[51.222.22.115]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00636-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00636-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing por WhatsApp con falso concurso de Copec	
Alerta de seguridad cibernética	8FPH22-00637-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022
Indicadores de compromiso	
URL sitio falso	
http://classificationcriterion.cn/empresascopec/tb.php?wy=mh1667900210206	
https://8yue22.cn/PkkfZcpa/empresascopec/?_t=1667908737331#1667908740560	
IP	
[104.21.77.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00637-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00637-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing por Whatsapp, que suplanta a Copec	
Alerta de seguridad cibernética	8FPH22-00638-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022
Indicadores de compromiso	
URL sitios falsos	
http://adventurerportrayal.cn/empresascopec/tb.php?hn=mt1667902051612	
https://8yue22.cn/6tpzpPYM/empresascopec/?_t=1667909914295#1667909921437	
IP	
[104.21.77.105]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00638-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00638-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00639-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022
Indicadores de compromiso	
URL redirección	
https://servistado.info/Solicitud_Aprobada/cuenta-kicl/	
URL sitio falso	
https://pr3sentamosweb.site/1667912467/imagenes/_personas/home/default.asp	
IP	
[47.87.151.212]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00639-01/	
https://www.csirt.gob.cl/media/2022/11/8FPH22-00639-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas en el Update Tuesday de Microsoft para Nov. 2022	
Alerta de seguridad cibernética	9VSA22-00740-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de noviembre de 2022
Última revisión	8 de noviembre de 2022

CVE

CVE-2022-23824	CVE-2022-41057	CVE-2022-41097
CVE-2022-37966	CVE-2022-41058	CVE-2022-41098
CVE-2022-37967	CVE-2022-41060	CVE-2022-41099
CVE-2022-37992	CVE-2022-41061	CVE-2022-41100
CVE-2022-38014	CVE-2022-41062	CVE-2022-41101
CVE-2022-38015	CVE-2022-41063	CVE-2022-41102
CVE-2022-38023	CVE-2022-41064	CVE-2022-41103
CVE-2022-39253	CVE-2022-41066	CVE-2022-41104
CVE-2022-39327	CVE-2022-41073	CVE-2022-41105
CVE-2022-41039	CVE-2022-41078	CVE-2022-41106
CVE-2022-41040	CVE-2022-41079	CVE-2022-41107
CVE-2022-41044	CVE-2022-41080	CVE-2022-41109
CVE-2022-41045	CVE-2022-41082	CVE-2022-41113
CVE-2022-41047	CVE-2022-41085	CVE-2022-41114
CVE-2022-41048	CVE-2022-41086	CVE-2022-41116
CVE-2022-41049	CVE-2022-41088	CVE-2022-41118
CVE-2022-41050	CVE-2022-41090	CVE-2022-41119
CVE-2022-41051	CVE-2022-41091	CVE-2022-41120
CVE-2022-41052	CVE-2022-41092	CVE-2022-41122
CVE-2022-41053	CVE-2022-41093	CVE-2022-41123
CVE-2022-41054	CVE-2022-41095	CVE-2022-41125
CVE-2022-41055	CVE-2022-41096	CVE-2022-41128
CVE-2022-41056		

Fabricante

Microsoft

Productos afectados

Azure CLI
Azure CycleCloud 7
Azure CycleCloud 8
Azure EFLOW
Azure RTOS GUIX Studio
Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.8.1

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 Business Central 2022 Release Wave 1
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.3
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Nuget 2.1.2
Nuget 4.8.5
SharePoint Server Subscription Edition Language Pack
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems

Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022 Datacenter: Azure Edition (Hotpatch) Windows Subsystem for Linux (WSL2) Windows Sysmon
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00740-01/
https://www.csirt.gob.cl/media/2022/11/9VSA22-00740-01.pdf

CSIRT comparte vulnerabilidades que afectan a productos de Cisco	
Alerta de seguridad cibernética	9VSA22-00741-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
CVE	
CVE-2022-20867 CVE-2022-20868 CVE-2022-20961	CVE-2022-20956 CVE-2022-20951 CVE-2022-20958
Fabricante	
Cisco	
Productos afectados	
Cisco ESA Cisco Secure Email and Web Manager Cisco Secure Web Appliance Cisco Identity Services Engine (ISE) Cisco BroadWorks CommPilot Application Software	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00741-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00741-01.pdf	

CSIRT comparte vulnerabilidades en Workspace ONE Assist solution	
Alerta de seguridad cibernética	9VSA22-00742-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	9 de noviembre de 2022
Última revisión	9 de noviembre de 2022
CVE	
CVE-2022-31685 CVE-2022-31686 CVE-2022-31687	CVE-2022-31688 CVE-2022-31689
Fabricantes	
VMware	
Productos afectados	
VMware Workspace ONE Assist 21.x y 22.x. Las vulnerabilidades son parchadas en la versión 22.10.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00742-01/	
https://www.csirt.gob.cl/media/2022/11/9VSA22-00742-01.pdf	

IoC - Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT de Gobierno.

El CSIRT de Gobierno 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	Tipo Malware	Documento web
33c1a387b8118c12cea6fc5c2673c94a52403e945ba76ac3dbb3a8c4649035f0	Emotet	2CMV22-00374-01
f794589c2b118c53894a21943813b43d95b5f9bef158dbda283a8859a7246254	Emotet	2CMV22-00374-01
cf2ca104cce3798296b220e3ea0b749c089dc10011531e0012c0a41a95c7b5d3	Emotet	2CMV22-00374-01
b07e769f7508a2e1d35f7d4835893051a08586d33192e4b933d36b0ecb4887f1	Emotet	2CMV22-00374-01
ce868c3cd85acb99df28599fec809e3af99292f996755dbad8038118201bedd0	Emotet	2CMV22-00374-01
b9eee623a848474899bf25709dc654346c764143d45038ef055220da70119f0f	Emotet	2CMV22-00374-01
b56305f0d32be944614288f8c27c4410d242eebcf87259cddcf687a37d179f1d	Emotet	2CMV22-00374-01
d86e1e56338a16cc1789ce68ed1996c2188cc4764f431e16390c46aef791c569	Emotet	2CMV22-00374-01
370c9603bb9b454372070ee671a62772a69729cb08ac7b58aee51583d7b7f3f0	Emotet	2CMV22-00374-01
ce1df5f23e6126202dc5c2e20b47168c6a06ecab2bebfb71a545d1a800cf0a43	Emotet	2CMV22-00374-01
0740ce43cd29acaf8cb96fdbfe414c5a614d953552a5c5cc1faa040465def06e	Emotet	2CMV22-00374-01
55501764c7388762cb3621027575be215529a78e2d296d6405e24dfccf16c29e	Emotet	2CMV22-00374-01
197a43730f3ff494f025bdd4435a3f92138cb1a85e488507f3f7a31bac368573	Emotet	2CMV22-00374-01
6fc6e50b0d7bedc713908a49db41b4157b6a4016c2be073aa1cbdda824b18643	Emotet	2CMV22-00374-01
25fce5f66196997fbbd2991df77a1b035aeef47b7d7f3139aa078b46b000bcbf	Emotet	2CMV22-00374-01

URL	Documento web
http://www.detertecnica[.]com/var/azLISfW/	2CMV22-00374-01
http://demo.cansunoto[.]com/lYqTuQ0qe5r2Y/	2CMV22-00374-01
http://cybertech.freeoda[.]com/ct/go6hL733p4vjEnuu/	2CMV22-00374-01
http://danoblab[.]com/wordpress_4/Fw/	2CMV22-00374-01
http://eznetb.synology[.]me/@eaDir/7ks2a6g9TV/	2CMV22-00374-01
http://www.chawkyfrenn[.]com/icon/BzGzSWFZIZGaTK/	2CMV22-00374-01
http://royreid.co[.]uk/wp-content/UIa3o/	2CMV22-00374-01
http://www.muyehuayi[.]com/cmp/Vtm2m7z88g/	2CMV22-00374-01
http://ly.yjlianyi[.]top/wp-admin/NRAdJ/	2CMV22-00374-01
http://ftp.agir-santeinternationale1[.]com/doctors/KAacngW97n4ApzVBDdGy/	2CMV22-00374-01

Actualidad

Alerta de Seguridad Cibernética | Parche para vulnerabilidades día cero en Microsoft Exchange Server

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, informa que Microsoft finalmente ha publicado parches para dos vulnerabilidades de día cero (CVE-2022-41040, que falsifica solicitudes del lado del servidor; y CVE-2022-41082, permite la ejecución remota de código (RCE) cuando el atacante logra acceder a PowerShell), conocidas en septiembre y apodadas ProxyNotShell, las cuales afectan a los servidores Exchange en sus versiones 2013, 2016 y 2019.

Es necesario que los encargados de ciberseguridad de las instituciones implementen estas actualizaciones cuanto antes. La información entregada por Microsoft para la descarga e instalación de los parches se encuentra aquí, aunque también se señala que son parte de la más reciente actualización de Windows Update:

https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d

El CSIRT de Gobierno compartió, durante octubre, noticias y mitigaciones relativas a las vulnerabilidades CVE-2022-41040 y CVE-2022-41082, documentos que pueden ser revisados en:

https://www.csirt.gob.cl/noticias/10cnd22-00084-01/

https://www.csirt.gob.cl/noticias/10cnd22-00084-02/

https://www.csirt.gob.cl/noticias/10cnd22-00084-03/

https://www.csirt.gob.cl/noticias/10cnd22-00084-04/

https://www.csirt.gob.cl/noticias/10cnd22-00084-05/

Ciberdiccionario Volumen 22

Esta semana compartimos nuestra edición número 22 del ciberdiccionario. En esta ocasión, explicamos qué son adware, egosurfing, metaverso y emotet.

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.

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 campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Gonzalo Ramírez
- Moisés Faguas
- Gabriela Valdivia
- Yanina Quilacan
- Juan Génova