Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

01-04-2021 | Año 3 | N°91

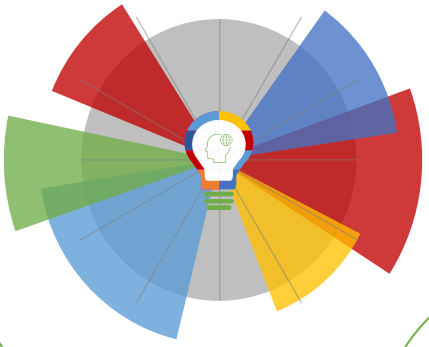
Boletín de Seguridad Cibernética

Semana del 26 al 31 de marzo de 2021

La semana en cifras

Hash
57
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
1
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
16
para vulnerabilidades
Las mitigaciones son útiles para productos de SolarWinds, Google y OpenSSL.

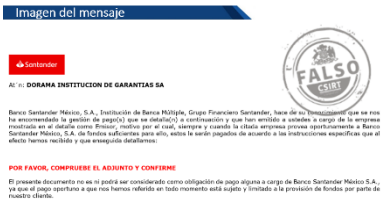
IP
50
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Malware

Imagen del mensaje

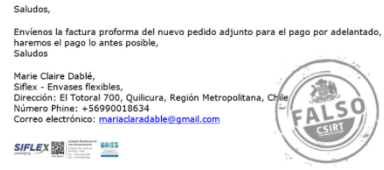


CSIRT alerta por campaña de malware suplantando a Banco	
Alerta de seguridad cibernética	2CMV21-00158-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2021
Última revisión	30 de marzo de 2021
Indicadores de compromiso	
SHA256	
69F8384DEA7A61D574FC76EFCE0F9DB1F942F58902A2AAA4211AB3A64C6A8878 BFFB6237B283938B6110DCE1F8FED7C298DD381AC9EA3A92C849E440F254511B	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00158-01/	

Imagen del mensaje

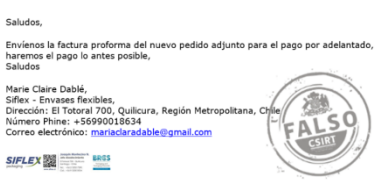
CSIRT alerta por campaña de malware con falsa orden de compra	
Alerta de seguridad cibernética	2CMV21-00159-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de marzo de 2021
Última revisión	30 de marzo de 2021
Indicadores de compromiso	
SHA256	
87A90A46CEE92BC5DD281628F12B2431FC418F3EAB21AFB6BDE86D59D470CA5B	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00159-01/	

Imagen del mensaje



CSIRT alerta por campaña de malware con factura falsa	
Alerta de seguridad cibernética	2CMV21-00160-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2021
Última revisión	31 de marzo de 2021
Indicadores de compromiso	
SHA256	
46772EF430645CB795EC68328B68AE2E3E380BB692596D4FE00DC0CC09F0C717 B4B5E6482B3D938EE19066DEB66EE9E886404BE87DBF0C9BD74B5833CFAFB2E7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00160-01/	

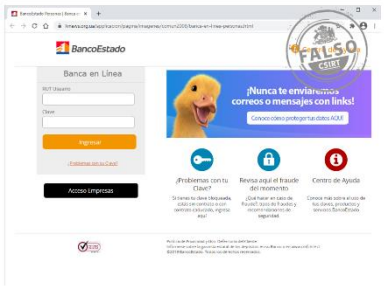
Imagen del mensaje



CSIRT alerta por campañas de phishing y comparte IOC para monitoreo	
Alerta de seguridad cibernética	2CMV21-00160-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2021
Última revisión	31 de marzo de 2021
Indicadores de compromiso	
SHA256	
46772EF430645CB795EC68328B68AE2E3E380BB692596D4FE00DC0CC09F0C717 B4B5E6482B3D938EE19066DEB66EE9E886404BE87DBF0C9BD74B5833CFAFB2E7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00160-01/	

Sitios fraudulentos

Imagen del sitio



CSIRT alerta por web fraudulenta que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FFR21-00925-01
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 2021
Última revisión	31 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://lvnews.org[.]ua/applicacion/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[195.201.34.52]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00925-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00925-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en SolarWinds Orion	
Alerta de seguridad cibernética	9VSA21-00413-01
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 2021
Última revisión	29 de marzo de 2021
CVE	
CVE-2021-3109 CVE-2021-35856 Pendiente Pendiente	
Fabricante	
SolarWinds	
Productos afectados	
Orion Platform	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00413-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00413-01.pdf	

CSIRT alerta de serias vulnerabilidades en OpenSSL	
Alerta de seguridad cibernética	9VSA21-00414-01
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 2021
Última revisión	29 de marzo de 2021
CVE	
CVE-2021-3450 CVE-2021-3449	
Fabricante	
OpenSSL Project	
Productos afectados	
OpenSSL versiones 1.1.1x anteriores a 1.1.1k	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00414-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00414-01.pdf	

CSIRT alerta de vulnerabilidades de alto riesgo en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00415-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2021
Última revisión	31 de marzo de 2021
CVE	
CVE-2021-21194 CVE-2021-21195 CVE-2021-21196 CVE-2021-21197 CVE-2021-21198 CVE-2021-21199 También hay cuatro vulnerabilidades más que aún no cuentan con su propio CVE	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones de la 89.0.4389.0 a la 89.0.4386.113.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00415-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00415-01.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
15730e1d21f85849f2ebc73123128f8090caf2875031aece1e873f753f384ca9	2CMV21-00161-01
2c7d043ef1315e5fe82e0dfb32c2a1c2d6d73251b6269283908df0f46340c128	2CMV21-00161-01
46772ef430645cb795ec68328b68ae2e3e380bb692596d4fe00dc0cc09f0c717	2CMV21-00161-01
4c72f894b1f77f39a841ea11ab8572d81c3fd525e78ceacf4b4cad4234aed667	2CMV21-00161-01
533a44c34e8c2e3363cdd8cd4da7400d55d0642ed7a00c31fc448f769532c6e0	2CMV21-00161-01
5fbedda881ce3eb91a839ccd4215d1caf22cf4f1295681ac303277688beb1f1d	2CMV21-00161-01
69f8384dea7a61d574fc76efce0f9db1f942f58902a2aaa4211ab3a64c6a8878	2CMV21-00161-01
6e51f766d318169ef070c77c7a1ee09284c8d6b3223cca08aa514acde6856e05	2CMV21-00161-01
79d315e7bbf748dae57c0f5da69997de76df1c99b82b3ac8c22eb8ef98e188dc	2CMV21-00161-01
7dc7244e1b2fb0730881cc0dc7c3dfcadfd683e57d4f08e8ea26ce5ca4e9ed90	2CMV21-00161-01
85bc6624c9e44abc68ac6cba4760fec0b3384721954e2419eb6d3f8e86ae300a	2CMV21-00161-01
87f4a7aae17466cfe271d8d1389e2ece68d497218590179e32c189292e910efa	2CMV21-00161-01
9197636d1d6a324534aae7c13305fb10a421e5bfe579eb9929cd1b3e1f174b6c	2CMV21-00161-01
a68f9d2f10ffa3d46d3c5f2f8a673eb8910dc00a30c3b1f06d92bc7f80e91600	2CMV21-00161-01
a802f1405d05351dcaec66458fde76740a3d37c23ece666439d1a25d8bb9fb11	2CMV21-00161-01
afa742615635ebe941e8b3609e3eda046bf4e9b9494cc18609c40d4e416111d7	2CMV21-00161-01
b342c20f7a99734ce6f49ec432d155e760c09d4bb264e54736bffa55e992ddbb	2CMV21-00161-01
c16a4eb88fc1ff28dc111479d0458f1268a909fc1354ae279ffde8f4dc32219c	2CMV21-00161-01
c3b550e62986878230e04940a7503a684ecc95c9c0ae764a806892170f94a8e8	2CMV21-00161-01
c5e1e50d3fdf47624ab94d1aaa1373ab05c841e64242dfba4b03a2980b234304	2CMV21-00161-01
c7accb573b13bd9b786063b2d586f779c57d00a01ba6e7e4c2262c52a397a48d	2CMV21-00161-01
d009bf653901f3f56cfe36ed4e724422fa1a0f16eb5175ed8a66d8ca82594239	2CMV21-00161-01
dcf080025c78b8a4aa12e3a96834e5cbac015b8be178a400a0836d8cbb292df0	2CMV21-00161-01
de8b95c67562881fe0e5bcb2e22b673d0acbdb8a848d0c3f835b28237e52d546	2CMV21-00161-01
e4c37c77632e0ac493520a7c4dc3f56cd22a5b40e51f890643544f1044803c10	2CMV21-00161-01
e67d88b394e780c4c96d4f49583d73fd383b051e967736696509d766329a1d0a	2CMV21-00161-01
e8c21beda9b685209b0017fd413cc807d30fea80b18f112c19baf0fdb42dee9d	2CMV21-00161-01
ec1cc9e522caef5f608aa965d33671e142d5cf801deef50d31cfe4755a4e71cc	2CMV21-00161-01
f3343704cbf630ed889003d45e94b81794cf64021fba0c6b907846c4c98c83f9	2CMV21-00161-01

fc026ebe0a13bd1b0a0ee4b66e0ebc869db554427e6dd17217f1b3e527e82ae2	2CMV21-00161-01
6248fc91bb54d50f768eb1c8d14e3c4578db3ad523366087ccd31573945bfebc	2CMV21-00162-01
a4b2c08ccb475bdd4767c584f58ca515b8991e7c9313fe2cc3c7329b47dc40c1	2CMV21-00162-01
232a1c5556532af6e20b5e65e7cf000e5421087a34b950cfae9bb7f447ce5b85	2CMV21-00162-01
d10cd82234dfee0db61da4b2b926f72fe9ddb1a0cc419a6f05dabba4713f3f5c	2CMV21-00162-01
6635a9c25337bda4dc01889593c315a5e403f8b836bdce53f7a24754a87964a2	2CMV21-00162-01
bbcbee39666d57e0d33de6342d3b7121580c7329ace9efbf3d0f1ac1132b0401	2CMV21-00162-01
bb881851c401f18651d160438cc157a01d27640b081b7b8c909b222986948682	2CMV21-00162-01
e1ceeb941c48b94b61f79ead85c5a9a0d1f59bf61246896d039eff1e8e45ece8	2CMV21-00162-01
7b5a54a62c235899394105a4e3535c192c4b8e9411d3a581896068cbcc2c5ee1	2CMV21-00162-01
cd315439089bed5676f19ac3eaae192497d36a5ecc5419ec783afb7440ac17fe	2CMV21-00162-01
cbb0deccf2474c13cab50f41c9123e620d04f9885caddf362a6086ddef612414	2CMV21-00162-01
f7262794ca21455693f2e119c4cb599a8b703466b10f37d8e5e9f4f64ad01985	2CMV21-00162-01
fc6595e4e5a56e7cdd65d5911c7d4e6af0a2988a4e0573160bd34a9267e646a0	2CMV21-00162-01
8a03c6d753d51cbbf8aff4a1ef51421ebd6e4e1dd0b6cc061e84a66cf867c13c	2CMV21-00162-01
af868fb563094032a83b34c6ee8385530895af9d9f4ccfd0b738077f78292c50	2CMV21-00162-01
496685dad6f66c09941f2a5564851e37bb661396946acb28d90528faea9d3d95	2CMV21-00162-01
5eaaa45ed003f11448fb8102ef54bf4404624bd44d4051c7fe5264bb029d00b3	2CMV21-00162-01
cca2fa3dce434ae716e051f092befd0337831885bd61d74c1fe2ebff371b6a89	2CMV21-00162-01
8710067e398716395453ba85af1d24f271e1a0c6b693c0b0382f1131f8c8392a	2CMV21-00162-01
702d344c9c803888dc4700804f96d882a54843915592ba1ef7ba387c7a81fbdc	2CMV21-00162-01

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
37.26.26.71	Uninet	2CMV21-00161-01
211.219.248.163	Korea telecom	2CMV21-00161-01
192.185.55.25	Unifiedlayer-as-1	2CMV21-00161-01
104.47.38.50	Microsoft-corp-msn-as-block	2CMV21-00161-01
93.39.109.35	Fastweb	2CMV21-00161-01
79.10.124.244	Telecom italia	2CMV21-00161-01
112.25.159.234	China mobile communications corporation	2CMV21-00161-01
185.78.85.242	Survivor bilisim teknolojileri a.s.	2CMV21-00161-01
192.185.145.3	Unifiedlayer-as-1	2CMV21-00161-01
199.127.218.11	Apyli-as	2CMV21-00161-01

45.62.234.199	Datacity	2CMV21-00161-01
103.137.212.5	Rainbow network limited	2CMV21-00161-01
221.115.191.113	Arteria networks corporation	2CMV21-00161-01
45.133.1.141	Des capital b.v.	2CMV21-00161-01
45.137.22.138	Rootlayer web services ltd.	2CMV21-00161-01
159.89.171.146	Digitalocean-asn	2CMV21-00161-01
37.252.96.159	Comvive servidores s.l	2CMV21-00161-01
168.235.110.64	ramnode	2CMV21-00161-01
189.50.50.10	Total telecom ltda-me	2CMV21-00161-01
101.36.119.223	Ucloud information technology (hk) limited	2CMV21-00161-01
151.73.90.69	Wind tre s.p.a.	2CMV21-00161-01
37.49.225.182	Peenq.nl	2CMV21-00161-01
91.64.208.212	Vodafone gmbh	2CMV21-00161-01
84.38.133.114	Dataclub s.a.	2CMV21-00161-01
134.209.64.219	Digitalocean-asn	2CMV21-00161-01
212.86.101.131	Zomro b.v.	2CMV21-00161-01
2.32.92.118	Vodafone italia s.p.a.	2CMV21-00161-01
196.203.86.28	Tunisia backbone as	2CMV21-00161-01
178.128.79.66	Digitalocean-asn	2CMV21-00162-01
98.254.192.194	Comcast-7922	2CMV21-00162-01
37.49.225.152	Peenq.nl	2CMV21-00162-01
89.72.216.89	Liberty global b.v.	2CMV21-00162-01
103.217.111.159	Dot internet	2CMV21-00162-01
103.133.111.8	Vietnam posts and telecommunications group	2CMV21-00162-01
73.129.131.230	Comcast-7922	2CMV21-00162-01
203.146.252.145	Cs loxinfo public company limited	2CMV21-00162-01
102.159.85.81	Topnet	2CMV21-00162-01
2.226.201.169	Fastweb	2CMV21-00162-01
165.232.176.203	Digitalocean-asn	2CMV21-00162-01
185.222.58.138	Rootlayer web services ltd.	2CMV21-00162-01
185.222.57.200	Rootlayer web services ltd.	2CMV21-00162-01
103.153.183.156	Snthostings	2CMV21-00162-01
219.122.9.188	Equinix japan enterprise k.k.	2CMV21-00162-01
95.215.206.12	Zomro b.v.	2CMV21-00162-01

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

Dirección	Documento web
abwlemy@fargoforecast.com	2CMV21-00161-01
ci@fargoforecast.com	2CMV21-00161-01
ckaefcu@fargoforecast.com	2CMV21-00161-01
davidb.jackson@hammondtractor.com	2CMV21-00161-01
defdcridiv3@defense.tn	2CMV21-00161-01
dsnco.cl@gmail.com	2CMV21-00161-01
eromero@mmr.com.pe	2CMV21-00161-01
fredasekini09@gmail.com	2CMV21-00161-01
gaurav@fortunex1.com	2CMV21-00161-01
Lincoln.Atkinson@msc.com	2CMV21-00161-01
ljlep@fargoforecast.com	2CMV21-00161-01
mariaclaradable@gmail.com	2CMV21-00161-01
mitchell@demuntzoeker.be	2CMV21-00161-01
mohammed.ali@algharshobgroup.com	2CMV21-00161-01
Monica.Cavita@assistcard.com	2CMV21-00161-01
Nakis.Kassos@gmcg.global	2CMV21-00161-01
Niko.Barnett@msc.com	2CMV21-00161-01
ojsor@fargoforecast.com	2CMV21-00161-01
peter@vertexpc.com	2CMV21-00161-01
quickbooks@notification.intuit.com	2CMV21-00161-01
Ricky.Parry@msc.com	2CMV21-00161-01
rilzu@fargoforecast.com	2CMV21-00161-01
RoseGutierrez@gmail.com	2CMV21-00161-01
saleh@wonderinter.com	2CMV21-00161-01
sales@guang-qi.com	2CMV21-00161-01
shihad@alhakbanigroup.com	2CMV21-00161-01
tcymdyo@fargoforecast.com	2CMV21-00161-01
arturocascan@gmail.com	2CMV21-00162-01
wang@mamanatalie.com	2CMV21-00162-01
olivialee@kingcar.com.tw	2CMV21-00162-01
esther.yii@ascentautomotive.com.sg	2CMV21-00162-01
vsb@tassgroup.com	2CMV21-00162-01
sales@singcomm.com.sg	2CMV21-00162-01
cole@got2start.com	2CMV21-00162-01
hq@megafitness.eu	2CMV21-00162-01

cruu@hsbc.com.hk	2CMV21-00162-01
system@sent-via.netsuite.com	2CMV21-00162-01
thumano.cafetero@gopack365.com	2CMV21-00162-01

IoC Ataques de Fuerza Bruta

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

IP	Etiqueta de sistema autónomo	Documento web
45.227.253.115	Global Layer B.V.	4IIA21-00029-01
27.255.75.16	EHOSTICT	4IIA21-00029-01
5.188.206.246	Krez 999 Eood	4IIA21-00029-01
78.128.113.131	Miti 2000 EOOD	4IIA21-00029-01
185.24.233.76	Sternforth Ltd.	4IIA21-00029-01

Actualidad

CSIRT de Gobierno imparte charla de ciberseguridad a miembros de la FACh

Miembros del CSIRT de Gobierno, encabezados por nuestro director nacional Carlos Landeros, hicieron charlas de ciberseguridad a alumnos de la cátedra de Inteligencia de la Academia de Guerra Aérea de la Fuerza Aérea de Chile, revisando diversos temas técnicos y normativos y generando una ronda de preguntas y respuestas con los alumnos.

Estas iniciativas refuerzan la importancia de la colaboración entre distintas organizaciones y empresas para lograr entre todos tener un país más ciberseguro.

Los detalles pueden encontrarse aquí: https://www.csirt.gob.cl/noticias/csirt-fach/

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.

- Andrés
- Mario Misael Castillo Moreira
- Elizabeth Carolina Ahumada Ruiz