Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

26-03-2021 | Año 3 | N°90

Boletín de Seguridad Cibernética

Semana del 19 al 25 de marzo de 2021

La semana en cifras

Hash

24

SHA

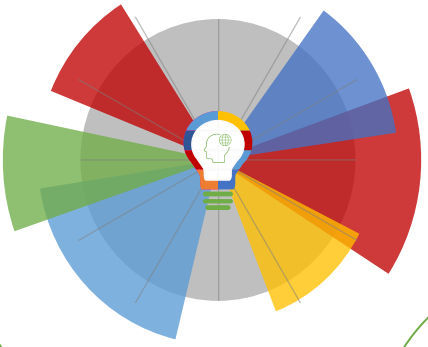
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

15

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

5

para vulnerabilidades

Las mitigaciones son útiles para productos de Mozilla y Adobe.

IP

23

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

Servicio de Impuestos Internos

FALSO CSIRT

Segundo Aviso:

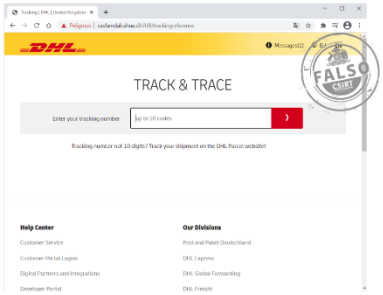
Fecha: 23-marzo-2021
Estimado:

El **Servicio de Impuestos Internos** se ha percatado que en diversos despachos alrededor del País, Ud. ha propuesto esquemas para **evadir el pago de impuestos** y hemos detectado **anomalías en su situación fiscal**. Para evitar una sanción en su contra que puede ser **una multa de hasta 50 UTM**, le recomendamos revisar su factura en el siguiente Enlace.

CSIRT advierte phishing con malware que suplanta al SII	
Alerta de seguridad cibernética	2CMV21-00157-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de marzo de 2021
Última revisión	24 de marzo de 2021
Indicadores de compromiso	
SHA256	
1C4FEB5B1CF3132C0B426F6FFC47E33B5E0EB163AFBC9DD1828B8546B94FF0F9 80DFB1D76D1F6E7BDB44E101EEC5F49FB6988FDA14A78B0E8689C361C93A2CCF 3A58CF08A6046804EA9F1CD262474C82DA2A249E41BF47534A48E2747BA69228	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00157-01/	

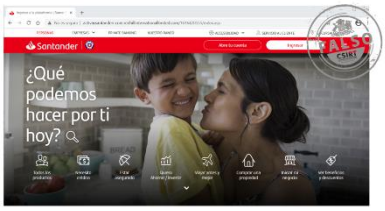
Sitios fraudulentos

Imagen del sitio



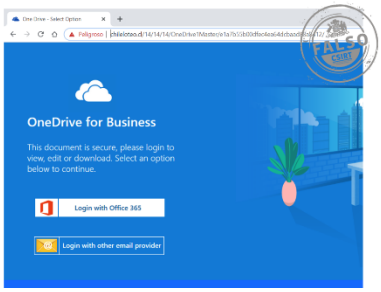
CSIRT alerta de una web fraudulenta que suplanta a DHL	
Alerta de seguridad cibernética	8FFR21-00920-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de marzo de 2021
Última revisión	19 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://cesfamdalcahue[.]cl/dhlll/trackingreference	
IP	
[186.64.119.225]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00920-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00920-01.pdf	

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a banco	
Alerta de seguridad cibernética	8FFR21-00921-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de marzo de 2021
Última revisión	22 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
http://activassantanderr.com.redhillinternationallimited[.]com	
IP	
[51.77.64.196]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00921-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00921-01.pdf	

Imagen del sitio

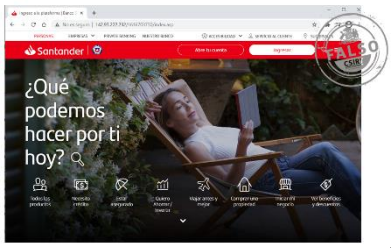


CSIRT advierte por sitio fraudulento que suplanta a OneDrive	
Alerta de seguridad cibernética	8FFR21-00922-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de marzo de 2021
Última revisión	22 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://chileloteo[.]cl/14/14/14/OneDrive1Master/e1a7b55b00dfec4ea64dcbaad88a8412/	
IP	
[66.232.107.218]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00922-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00922-01.pdf	

Imagen del sitio

CSIRT alerta por web fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00923-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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	
URL sitio falso	
https://www.loginsamtander.cl-cam[.]com/ab1f2d560b425011082998ee45a9782f/index.asp	
IP	
[104.219.248.73]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00923-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00923-01.pdf	

Imagen del sitio



CSIRT alerta por web fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00924-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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	
URL sitio falso	
http://142.93.222[.]232/1616703657/index.asp	
IP	
[142.93.222.232]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00924-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00924-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta ante campaña de phishing simulando ser banco	
Alerta de seguridad cibernética	8FPH21-00379-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de marzo de 2021
Última revisión	22 de marzo de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3c8uwnz?l=www.itau.cl http://wordpress.roma[.]it/favicon/enviar03.php?l=990694647 http://www.lacreatura.esivalladolid[.]com/activacion/cuenta-qqoq/	
URL sitio falso	
https://www.navigatorthailand[.]com/logs/www.itau.cl/pagina/index.php	
IP	
[119.59.104.10]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00379-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00379-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing suplantando al BancoEstado	
Alerta de seguridad cibernética	8FPH21-00380-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de marzo de 2021
Última revisión	23 de marzo de 2021
Indicadores de compromiso	
URL redirección	
http://citypawn[.]ca/activacion/cuenta-spli/	
URL sitio falso	
https://valpanet[.]com/ch3ch3r345s4u/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.117.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00380-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00380-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing suplantando al Banco Itaú	
Alerta de seguridad cibernética	8FPH21-00381-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
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	
URL redirección	
https://bit[.]ly/3raWGmh?l=www.itau.cl http://wordpress.roma[.]it/wp-admin/_notes/enviar.php?l=1001764909 http://www.lacreatura.esivalladolid[.]com/activacion/cuenta-eorq/	
URL sitio falso	
https://www.mdctscreen[.]com/bup1/www.itau.cl/pagina/index.php	
IP	
[200.23.37.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00381-01/	
https://www.csirt.gob.cl/media/2021/02/8FPH21-00381-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Mozilla Thunderbird	
Alerta de seguridad cibernética	9VSA21-00411-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de marzo de 2021
Última revisión	24 de marzo de 2021
CVE	
CVE-2021-23981 CVE-2021-23982 CVE-2021-23984 CVE-2021-23987	
Fabricante	
Mozilla	
Productos afectados	
Mozilla Thunderbird, versiones de la 60.0 a la 78.8.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00411-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00411-01.pdf	

CSIRT alerta de vulnerabilidad grave en Adobe ColdFusion	
Alerta de seguridad cibernética	9VSA21-00412-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de marzo de 2021
Última revisión	24 de marzo de 2021
CVE	
CVE-2021-21087	
Fabricante	
Adobe	
Productos afectados	
ColdFusion 2016, 2018 y 2021.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00412-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00412-01.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
0fc6d6629ca1b970a92cd0347565d91c5c8b0061507f7d2470539de5c3e2c6ee	2CMV21-00156-01
1f18fdc9c5c10e49bcfb4276df89ccc9c4cd2179051c5115614e01292100b820	2CMV21-00156-01
3015bc6aed4f82cb09384b63c3d54dc9dba61779090e202d8406921cb04f572b	2CMV21-00156-01
3e25fa3018ad1779d795f15e1f33b860dacc6766e88dcad606149034bcbc625e	2CMV21-00156-01
4dac8eab5516ae5dc0b0e32d312b8ebc65acd9f167c214dad181cdc7a2aa581e	2CMV21-00156-01
4df436a10e88a39872cbf427640598b98fb5fe9c93d46e579905587510b71d39	2CMV21-00156-01
77577648eb3f615670575f215638ffb9acd1d7f0fb864c2464e85a50f921416c	2CMV21-00156-01
7a450959435a0a7129fdf18239bd43ea163a32fb364142b639b807cef1707ffe	2CMV21-00156-01
836aec7caf8b90b52b177c3d80a56726400d0c9a94625d1e9158af02e9b362b1	2CMV21-00156-01
8c5d475a5b57f7b0c328f1d969de76704c95af8ebcfa671787784ebe476088e4	2CMV21-00156-01
94ee45d6ad8cfe944c069be62144f7d896f932ed43a3d26eeb6439ef9db3dbc8	2CMV21-00156-01
9786a923b8086c1bf402702ee73ef564f1ce2e1a1da503dfef2afa3a7a547c6f	2CMV21-00156-01
acb2b92c42fe35d16b98b26b2db43f7f944ce1dd160f60a00041f1359268a26d	2CMV21-00156-01
afd91f5be793a8e4bd724181bc6f3d7fd4a0a286e4d50c035cbbcf837380d0ef	2CMV21-00156-01
b10e064b4d2952b2e4a9e9a45314fc9a75a7ddb80c3af6b5a8549611a66b5bcc	2CMV21-00156-01
b648900cce5e5b4a8b375ee2fb601490fb03438770306a0d9dc6a52ee0a2e371	2CMV21-00156-01
bc81d4cd3de51226c9e25b6bdab6c18d564eb2b610c0f7f1fa3c003022d61c15	2CMV21-00156-01
c19736bbf12877b3467b647034054f491ad3505add4665e2e4b4114780904020	2CMV21-00156-01
c888202a2eeb11b0d181c4699119fba99a7f220065cf37f6247c9eb7df3a13eb	2CMV21-00156-01
dd55f956428248f5a30829cb0145764e3a7c551c741bc0bd653594c20678e283	2CMV21-00156-01
eebc2baa15f22e594883357165d3b1119daa417dbb5c9b4dcd81bc028f321397	2CMV21-00156-01

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
89.163.145.207	Myloc managed it ag	2CMV21-00156-01

103.141.138.124	Vietnam posts and telecommunications group	2CMV21-00156-01
103.156.91.170	Vietnam posts and telecommunications group	2CMV21-00156-01
134.122.15.115	Digitalocean-asn	2CMV21-00156-01
172.93.195.29	Nexeon	2CMV21-00156-01
185.222.57.162	Rootlayer web services ltd.	2CMV21-00156-01
185.222.58.104	Rootlayer web services ltd.	2CMV21-00156-01
185.222.58.106	Rootlayer web services ltd.	2CMV21-00156-01
185.74.4.8	Uzbektelekom joint stock company	2CMV21-00156-01
193.56.29.139	Web hosted group ltd	2CMV21-00156-01
23.83.133.137	Leaseweb-usa-phx-11	2CMV21-00156-01
37.49.225.171	Peenq.nl	2CMV21-00156-01
45.137.22.107	Rootlayer web services ltd.	2CMV21-00156-01
45.137.22.150	Rootlayer web services ltd.	2CMV21-00156-01
64.44.139.178	Nexeon	2CMV21-00156-01
74.208.120.53	1&1 ionos se	2CMV21-00156-01
85.114.39.210	Optima telekom d.d.	2CMV21-00156-01

Indicadores de compromiso asociados a vulnerabilidad en BIG-IP y BIG-IQ de F5

67.216.209[.]142	9VSA21-00410-01
68.183.179[.]130	9VSA21-00410-01
203[.]159.80.241	9VSA21-00410-01
112.97.56[.]78	9VSA21-00410-01
13.70.46[.]69	9VSA21-00410-01
115.236.5[.]58	9VSA21-00410-01

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

Dirección	Documento web
compras@quimicasagal.com	2CMV21-00156-01
accounts@jllshipping.ae	2CMV21-00156-01
accounts01@shipping.sinosteel.com	2CMV21-00156-01
ahmad.salah@nss-shipping.com	2CMV21-00156-01
avitaillement@gema-group.com	2CMV21-00156-01
compras@quimicasagal.com	2CMV21-00156-01
contactos@celhex.cl	2CMV21-00156-01
franclinesale@305.bnjo.cf	2CMV21-00156-01

hasan@syrabiagroup.com	2CMV21-00156-01
info@pramuk.net	2CMV21-00156-01
info@salek.ae	2CMV21-00156-01
mani@slettennorge.com	2CMV21-00156-01
pagoz@novafriolog.com	2CMV21-00156-01
purchases.adaltis@netease.com	2CMV21-00156-01
purchasing@qfautomation.com	2CMV21-00156-01
sales@mediamage.co.za	2CMV21-00156-01
samiya.khan@BarrettHodgson.com	2CMV21-00156-01
sumanta@themtech.co.th	2CMV21-00156-01
tuoint@phucthanh.com.vn	2CMV21-00156-01

Actualidad

CSIRT de Gobierno comparte una nueva edición de CiberSucesos centrada en la ingeniería social, de cara a la Operación Renta

La edición de marzo de la revista CiberSucesos se dedica a combatir el phishing y la ingeniería social, en el contexto de la Operación Renta, que cada abril atrae el interés de los ciberdelincuentes, que aumentan sus estafas digitales. En este contexto, contamos con los testimonios del director del Servicio de Impuestos Internos (SII) y la tesorera general de la República, quienes nos explican cómo se preparan para la enorme demanda que les genera la Operación Renta.

CiberSucesos no. 8 puede encontrarse aquí, para su lectura y descarga:
https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-8/

Ciberguía para la denuncia del acoso digital

Continuando con las actividades por el mes contra el ciberacoso y nuestra colaboración con la Fundación Katy Summer, compartimos una guía que explica paso a paso cómo denunciar las acciones de ciberbullying, tanto en las mismas plataformas de RR.SS. como ante la Policía de Investigaciones y el Ministerio Público.

La infografía completa en PDF, con todos los consejos, aquí:
https://www.csirt.gob.cl/recomendaciones/ciberguia-acoso-digital/

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.

- Lukas Isaac Abraham Lee Navarro
- Leandro Vivanco

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.26 14:09:12 -03'00'