Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

19-03-2021 | Año 3 | N°89

Boletín de Seguridad Cibernética

Semana del 12 al 18 de marzo de 2021

La semana en cifras

Hash

41

SHA

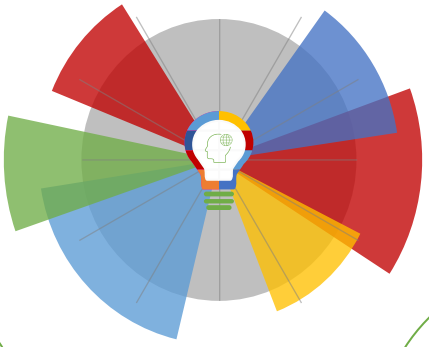
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

3

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

10

para vulnerabilidades

Las mitigaciones son útiles para productos de Google, Cisco y F5.

IP

38

Informadas

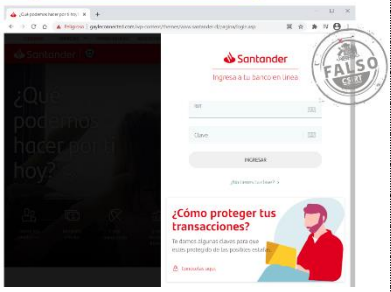
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

Imagen del sitio



CSIRT alerta página fraudulenta que suplanta a banco	
Alerta de seguridad cibernética	8FFR21-00917-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de marzo de 2021
Última revisión	12 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://gayleconnected[.]com/wp-content/themes/www.santander.cl/pagina/login.asp	
IP	
[18.133.103.41]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00917-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00917-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que imita a banco	
Alerta de seguridad cibernética	8FFR21-00918-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de marzo de 2021
Última revisión	12 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://validatarjeta-sms[.]live/1615578315/personas/index.asp	
IP	
[104.219.248.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00918-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00918-01.pdf	

Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta a banco	
Alerta de seguridad cibernética	8FFR21-00919-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de marzo de 2021
Última revisión	12 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://verifigsms-sntdr[.]website/1615581521/personas/index.asp	
IP	
[104.219.248.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00919-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00919-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades críticas en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00407-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2021
Última revisión	15 de marzo de 2021
CVE	
CVE-2021-21191 CVE-2021-21192 CVE-2021-21193	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones hasta la 89.0.4389.72.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00407-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00407-01.pdf	

CSIRT alerta de vulnerabilidades en productos BIG-IP de F5	
Alerta de seguridad cibernética	9VSA21-00408-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de marzo de 2021
Última revisión	16 de marzo de 2021
CVE	
CVE-2021-22987 CVE-2021-22988 CVE-2021-22990 CVE-2021-22992 CVE-2021-23000 CVE-2021-23003	
Fabricante	
F5	
Productos afectados	
BIG-IP, versiones de la 11.6.1 a la 16.0.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00408-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00408-01.pdf	

CSIRT advierte de vulnerabilidad grave en algunos routers de Cisco	
Alerta de seguridad cibernética	9VSA21-00409-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de marzo de 2021
Última revisión	18 de marzo de 2021
CVE	
CVE-2021-1287	
Fabricante	
Cisco	
Productos afectados	
Routers RV132W ADSL2+ Wireless-N VPN Routers RV134W VDSL2 Wireless-AC VPN	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00409-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00409-01.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
3bc245433cdc0ed5b755643239cce535879f36033baca71372a6bc5f520bdfb9	2CMV21-00154-01
3f527f6b74eb3aa050429314104c43d2436fab38e7cf70ab72db9304ca4167eb	2CMV21-00154-01
45b5ea8ca473975c84528216c08fffbf08883f289c6860cdb9b6f94521909dbc	2CMV21-00154-01
6d507c5f16b5a8bcef7cc715a2693cc83b240563df47e9c37f744eaa6bfbbf61	2CMV21-00154-01
703ba0d3604d3d88b0305c354eb596f5a946b1cda30a4b6e5cd524cb8012afe5	2CMV21-00154-01
753cbae11a881b871e3295d65449954817061db5dec53df7b379fee9f21c33d1	2CMV21-00154-01
7a2811fe02a2edf89723521cd1562aa6bb383918820df3fe01f87020f98f296d	2CMV21-00154-01
7f22df3a8aca7f8a184f063bbab3de9bfdf3c10c09bf95ee54eab5c8090752e9	2CMV21-00154-01
85beebafb964a562f652d048c758a3d6ee0c9a2c1f847944b53c965b679e336e	2CMV21-00154-01
93d935495f7f40deaf07b68afea7d4c953e14914a28b10412498ccd26fa859bb	2CMV21-00154-01
a1159d62fcb4dcb363be830e689a3872a70e7e71c71c44fabc478ba8dec3b31b	2CMV21-00154-01
a908ebece5fbe0931bc9be0c7330bafe25f67ade21cba15bb5bab101ccfb5963	2CMV21-00154-01
adae3a7030b466563ad42ebcdf174b6ac89928a2e50e3697a40a4bf007495c29	2CMV21-00154-01
b58acc04c92d4df0432f66dcc5721501b7e9c1cc486143e0badf42adec836d84	2CMV21-00154-01
c23d659803615497f1f9a01af5eb6763505687dd61845749a0dc6e16c9d477fd	2CMV21-00154-01
caecde573eb1b31ce10a947c2471178e006f99055aa40493eb234d1ce07190ec	2CMV21-00154-01
cbe045e37356a0d9b86655b93fcda9cab0ce16ab4d39c01fecfbca301b6032b1	2CMV21-00154-01
d25247dc5c3c487deffe3e7c04833d569136ce6051a6e9dd63d327ded974d704	2CMV21-00154-01
d578337ed0975cfd23f3edf0544281e226ff04bed93ce4e76cf7ba9683a9c420	2CMV21-00154-01
d7b0b24695fedabd57e8311ef54ca3a18b38a417508e2d2117707b371373ebb3	2CMV21-00154-01
e3e38dd48e944f70e5cf324d557ddfd48d7e66d4150a28e88a49dc4e9424565b	2CMV21-00154-01
eca1e93dc48c110cf049c081ba17fa0bc61560896e0dd19fe655aa45156e2b77	2CMV21-00154-01
f0a6419a2c90ff826169070629240cbbe573b3aff655e6bf4c06387e2fbe94ba	2CMV21-00154-01
f4ea1ec8a9feaa61cfb94f41750aa140d0b972ff7a8cd092eafcae9b89600650	2CMV21-00154-01
f79bb4189ba2ddd3107a8bbc6ac74380c6677a850373255a8bfb32b96fbc0ab8	2CMV21-00154-01
f8b9d8abdab8eb76a376013e55887bfcda18664d7e73ca42e97ffda183d128f1	2CMV21-00154-01
0ae37749d736d3a6dc155c5aa0a43af79c31d2f9165b862a03b00cd64e622c35	2CMV21-00155-01
19d9bc16e7bae6ba8231060d7894ed0f6aca9ddbe628bf3f5885a10fda2c4694	2CMV21-00155-01
2e2f814cb371d2f05136842a8e002702279b061bdb98b576de2f56f32afc3a2e	2CMV21-00155-01
3468cda4f6d72b10b55f969fbbc5633ffe6bbbc3615c7d529093929f05d5a3a5	2CMV21-00155-01

359491d123c2f0b7a4ce3053851af5ccd0616aa973260bb2f89d6e6c05a92b8d	2CMV21-00155-01
4c114775c104cae42034919a2409785b6f460245469777db72fff8c65e7b497a	2CMV21-00155-01
6b420fccd0de12888f901e34db6061d2e1d87263c06bbd04253f4dc85b383241	2CMV21-00155-01
6d182df081f770397f138e93a95114151dce0e89cb761238ce179471d9b54598	2CMV21-00155-01
6f43bf65070c99e87c0f97ec7945aeb1b110034347f74f56d99ab3915e5d81b2	2CMV21-00155-01
a875f5227631bb3f7a9482ec128bc9b5ec8e653a9b253d349c6e607bdc44dedd	2CMV21-00155-01
b504d0c6a3638563d7dcb5478c53e13ba3a3e1727c8780fafa445255fb223f20	2CMV21-00155-01
cd4cd0cb4effc3346bb53a4451f7e4c327b00d33faf9e0da1725ae62f0111795	2CMV21-00155-01
e70284cc39380d172a8837a0fed2f3c2947f80d10e26b96cfa46a60584e3dab6	2CMV21-00155-01
e916dffa6fc2d16debc047f4b4dabf66aa7fc7a611852ed0ccd074128d54e531	2CMV21-00155-01
f6bfaf84d404146f1024255af437c8c562fbe76f69e86f2dc2877aa5c99086c0	2CMV21-00155-01

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
87.126.174.11	Vivacom	2CMV21-00154-01
73.98.182.238	COMCAST-7922	2CMV21-00154-01
67.52.174.126	TWC-20001-PACWEST	2CMV21-00154-01
45.85.90.232	Des Capital B.V.	2CMV21-00154-01
31.214.176.32	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.31	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.29	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.27	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.26	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.25	Soluciones Corporativas IP, SL	2CMV21-00154-01
31.214.176.23	Soluciones Corporativas IP, SL	2CMV21-00154-01
207.7.86.108	PRIVATESYSTEMS	2CMV21-00154-01
192.249.122.78	INMOTION	2CMV21-00154-01
190.146.47.121	Telmex Colombia S.A.	2CMV21-00154-01
166.167.45.101	CELLCO	2CMV21-00154-01
124.29.202.102	Cyber Internet Services Pakistan	2CMV21-00154-01
108.175.14.66	1&1 Ionos Se	2CMV21-00154-01
107.167.82.209	IOFLOOD	2CMV21-00154-01
104.223.119.82	ASN-QUADRANET-GLOBAL	2CMV21-00154-01
103.99.1.144	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00154-01

85.214.160.219	Strato AG	2CMV21-00154-01
23.235.223.128	INMOTION	2CMV21-00154-01
195.242.110.186	Internet it company inc	2CMV21-00155-01
185.222.57.157	Rootlayer web services ltd.	2CMV21-00155-01
103.70.136.119	The value hosted (pvt.) Limited	2CMV21-00155-01
89.163.145.207	Myloc managed it ag	2CMV21-00155-01
185.222.57.162	Rootlayer web services ltd.	2CMV21-00155-01
195.201.121.93	Hetzner online gmbh	2CMV21-00155-01
128.199.26.39	Digitalocean-asn	2CMV21-00155-01
103.99.1.141	Vietnam posts and telecommunications group	2CMV21-00155-01
23.238.115.10	Hostwinds	2CMV21-00155-01
103.151.125.15	Vietnam posts and telecommunications group	2CMV21-00155-01

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

Dirección	Documento web
santander@venex.com.ar	2CMV21-00154-01
tzijuc@koepfamily.com	2CMV21-00154-01
sanjay.khan@bhm.co.in	2CMV21-00154-01
salesaci@arabiancrownintl.com	2CMV21-00154-01
sales023@bornsun.com.cn	2CMV21-00154-01
rochelle.ann@petnet.com.ph	2CMV21-00154-01
qojaluy@koepfamily.com	2CMV21-00154-01
oy@koepfamily.com	2CMV21-00154-01
no@koepfamily.com	2CMV21-00154-01
mohammed.shuji@oceanoil.com	2CMV21-00154-01
janzsys@koepfamily.com	2CMV21-00154-01
iucaybu@koepfamily.com	2CMV21-00154-01
ipysku@koepfamily.com	2CMV21-00154-01
ierexu@koepfamily.com	2CMV21-00154-01
hfeluyz@koepfamily.com	2CMV21-00154-01
ebwotko@koepfamily.com	2CMV21-00154-01
cs01@jandragon.com	2CMV21-00154-01
contact@gundersondenton.com	2CMV21-00154-01
circular@audicubic.com	2CMV21-00154-01
aqboled@koepfamily.com	2CMV21-00154-01
office@fokasibee.cyou	2CMV21-00155-01
rishav.pokharel@pkf.com.np	2CMV21-00155-01

noreply@hsbc-internationalwire.com	2CMV21-00155-01
info@epecuen.com.ar	2CMV21-00155-01
rebes01@tejidosrebes.com	2CMV21-00155-01
cberner@aldogroup.com	2CMV21-00155-01
Info@bgenergy.in	2CMV21-00155-01
info@colinbibra.com	2CMV21-00155-01
Gilana.mohamed@elserafy.com	2CMV21-00155-01
noreply@notify.ocbc.com.sg	2CMV21-00155-01
__cpanel__service__auth__icontact__hierbdimkhy1ncej@rs2.noc254.com	2CMV21-00155-01

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
87.246.7.244	Internet Hosting LTD	4IIA21-00033-01
193.169.255.72	GigaHostingServices OU	4IIA21-00033-01
212.70.149.55	Internet Hosting LTD	4IIA21-00033-01

Actualidad

Director nacional participa en artículo de La Tercera sobre vulnerabilidad en MS Exchange


Secciones LA TERCERA SUSCRÍBETE Inicio de sesión
Porque los hechos importan SUSCRÍBETE DESDE $990 AL MES
PULSO Ciberseguridad CMF

Alertas, protocolos y casos internacionales: cómo fue el incidente de ciberseguridad que sufrió la CMF

A inicios de mes el CSIRT había advertido sobre esta vulnerabilidad que requería parches para ser subsanada. La banca también lo tenía en el radar y había parchado sus sistemas con anterioridad. El sábado la industria se enteró oficialmente de la brecha que estaba afectando a la autoridad, por lo que se encendieron las alarmas. Fue el mismo que afectó a la Autoridad Bancaria Europea y al parlamento de Noruega.

El director nacional del CSIRT de Gobierno, Carlos Landeros, fue entrevistado por Mariana Marusic de La Tercera, instancia en la que explicó que el incidente anunciado por la CMF el domingo 14 de marzo correspondió, tal como a los ataques sufridos por el Parlamento de Noruega y la Autoridad Bancaria Europea, a servidores de correos comprometidos por vulnerabilidades de Microsoft Exchange.

Nuestro director también detalló que el ingreso no autorizado sufrido por la CMF aprovecha la vulnerabilidad de Microsoft Exchange, para hacerse pasar por alguien que tiene acceso autorizado al sistema, y que la CMF no es un blanco particular de esta campaña de ataques, sino que estos están afectando a diversas instituciones en todo el mundo, solo basta que tengan servidores de Exchange vulnerables.

La noticia completa, aquí: Alertas, protocolos y casos internacionales: cómo fue el incidente de ciberseguridad que sufrió la CMF - La Tercera.

Dia nacional contra el ciberacoso

Aprovechando que se conmemoró un nuevo día nacional contra el ciberacoso, decidimos compartir a través de nuestras redes sociales esta guía elaborada por el CSIRT de Gobierno, para que padres e hijos celebren un pacto que proteja a los menores en internet y ayude a prevenir el ciberacoso.

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

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.

- Karen Penroz Arias
- Catalina de los Ángeles Campusano Morales
- Roberto Carlos Bisquett Carmona
- Claudio Valderrama
- Fernando Flores Tobar
- Franco Tomás Sanllehi Romero

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.19 15:42:57 -03'00'