Ministerio del Interior y Seguridad Pública

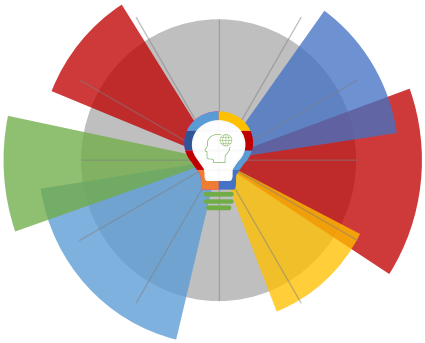
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

29-04-2022 | Año 4 | N°147

Boletín de Seguridad Cibernética

Semana del 22 al 28 de abril de 2022

La semana en cifras



Se advirtieron

13

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

73

para vulnerabilidades

Sus mitigaciones son útiles en productos de Cisco, Linux y Red Hat.

IP

5

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....2
Sitios fraudulentos....4
Phishing....6
Vulnerabilidades....7
Actualidad....10
Muro de la Fama....13

Malware

CSIRT advierte campaña de malware con falsa factura	
Alerta de seguridad cibernética	2CMV21-00294-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022

Indicadores de compromiso

SHA256

1da8317a526071257350676466059 1cc08833f958dd61e4c463ed58f7e2d80c6
de60b4ecb8edf8aa43ff5a88f2a9b7fcae285605c335bf008133234c6837b6c1
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967
bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f
fab1a6707cc62d923da3daf419d5c507b45f18de9935a36d0758f804fc628b7f
f8d14264a6498d478408e42a6c1607c8887afaa6734c9f1245ab14ced6bb1595
433d151da58380c7fb540810a3b6d4f39933cfeaaf771f79c23c07b70b0b1508
a392563e29ed18e6e8499f62d8b9c3325f13e7db6207ffab61874e4006e8e476
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

IoC URL

hXXps://ra.sav.us[.]es/.factura/?hash=
hXXps://facturaeletronica.northeurope.cloudapp.azure[.]com/2022/?hash=
hXXps://special.arabi21[.]com/russiaWP/EPSSubDirectoryBIN.zip

Enlaces para revisar el informe:

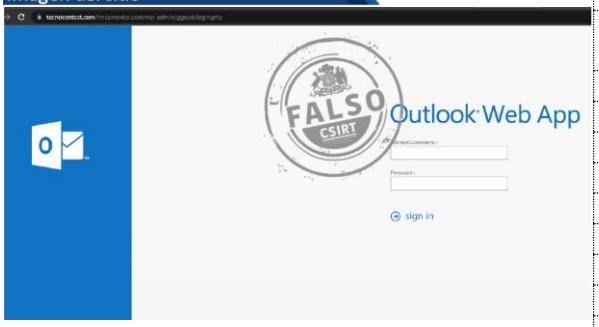
https://www.csirt.gob.cl/alertas/2cmv22-0294-01/
https://www.csirt.gob.cl/media/2022/03/2CMV22-00294-01.pdf

Imagen del mensaje

CSIRT advierte malware que suplanta a la TGR	
Alerta de seguridad cibernética	2CMV21-00295-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022
Indicadores de compromiso	
SHA256	
e13cce0cd9bd4f0854cc5413c7a55929155bfe2afe46247ee6763eb77635c645 2185765b437b0ac6b233605d00f8c98cb34c2e3154152522c02ee5c64d143ffc 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967 bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f 893ce8ba10a2c734921c1fe49219972fbb032dbcf7fb49d443031c639a4b21c4 cb6a6c3920daf4a5f84b89d80e9100f2dfbcec146ae3f4eefea526cf912aa086 728ec4e457500b7516fe73bbde00fbc4651db61961d666a235ef49b74154769f c76a16d7e5909031501bdb1f4860d9ba4be17cd054ca04547dd5d6fc5299410d 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4	
IoC URL	
hXXps://placade[.]jp/agt/–/https:/www.tgr.cl/?cliente= hXXps://www.stt.eesc.usp[.]br/wp-content/languages/Tgr0014220.zip hXXps://manuelruso[.]com/images/import/6xhj17x312dlk2hwe718.zip	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0295-01/	
https://www.csirt.gob.cl/media/2022/03/2CMV22-00295-01.pdf	

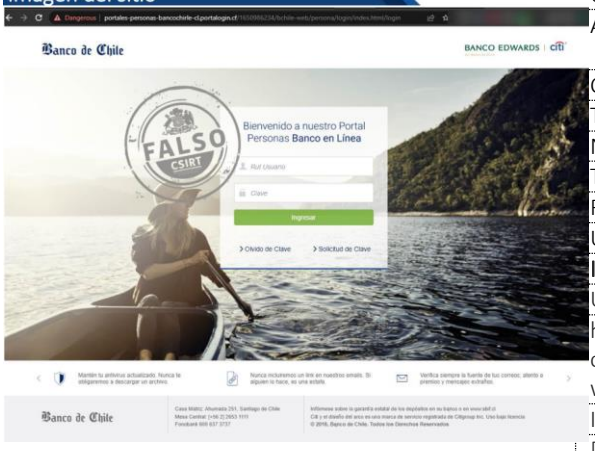
Sitios fraudulentos

Imagen del sitio



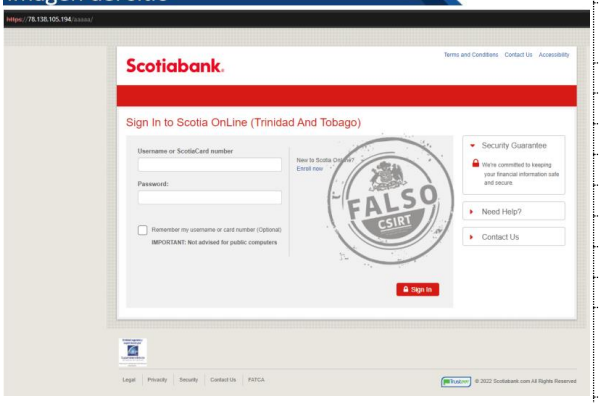
CSIRT advierte página web falsa de Outlook Web App	
Alerta de seguridad cibernética	8FFR22-01077-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2022
Última revisión	25 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://www.tecnocentest[.]com/imcamexico.com/wp-admin/ggusd/login.php	
IP	
[172.67.206.71]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01077-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01077-01.pdf	

Imagen del sitio



CSIRT informa página web que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01078-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2022
Última revisión	26 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://portales-personas-bancochirle-cl.portalogin[.]cf/1650986234/bchile-web/persona/login/index.html/login	
IP	
[172.67.203.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01078-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01078-01.pdf	

Imagen del sitio



CSIRT advierte sitio web que suplanta al banco Scotiabank	
Alerta de seguridad cibernética	8FFR22-01079-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://portales-personas-bancochirle-cl.portalogin[.]cf/1650986234/bchile-web/persona/login/index.html/login	
IP	
[78.138.105.194]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01079-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01079-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing con falsos puntos del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00515-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de abril de 2022
Última revisión	22 de abril de 2022
Indicadores de compromiso	
URL redirección	
hXXp://ec2-3-88-200-149.compute-1.amazonaws[.]com/CL-001293129317/?hash=ZHp1cml0YUBpbnRlcmlvci5nb3YuY2w=	
URL sitio falso	
hXXps://itaupuntos[.]net/726a292db52f7f5/html/index.php	
IP	
[44.203.5.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00515-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00515-01.pdf	

Imagen del mensaje

CSIRT informa phishing con falso monto aprobado del Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00516-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2022
Última revisión	25 de abril de 2022
Indicadores de compromiso	
URL redirección	
hXXps://bit[.]ly/3v1ErVC?l=www.bancoripley.cl hXXps://www.clmedicalltd[.]com/wp-content/languages/plugins/enviar.php?l=666704876 hXXps://wardatalwadirealestates[.]com/activacion/cuenta-ljei/	
URL sitio falso	
hXXp://www-bancoripley.cl.workhost[.]in/1650898777/login	
IP	
[94.130.8.49]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00516-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00516-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades en productos de Red Hat	
Alerta de seguridad cibernética	9VSA22-00624-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022

CVE

CVE-2022-29599	CVE-2022-25636	CVE-2022-25173
CVE-2021-44716	CVE-2022-22965	CVE-2022-25174
CVE-2022-21426	CVE-2021-4028	CVE-2022-25175
CVE-2022-21434	CVE-2021-4083	CVE-2022-25176
CVE-2022-21443	CVE-2021-20288	CVE-2022-25177
CVE-2022-21476	CVE-2021-43859	CVE-2022-25178
CVE-2022-21496	CVE-2021-45960	CVE-2022-25179
CVE-2021-4083	CVE-2021-46143	CVE-2022-25180
CVE-2022-0492	CVE-2022-0778	CVE-2022-25181
CVE-2022-25636	CVE-2022-22720	CVE-2022-25182
CVE-2021-4083	CVE-2022-22822	CVE-2022-25183
CVE-2022-0492	CVE-2022-22823	CVE-2022-25184
CVE-2022-21426	CVE-2022-22824	CVE-2022-25235
CVE-2022-21434	CVE-2022-22825	CVE-2022-25236
CVE-2022-21443	CVE-2022-22826	CVE-2022-25315
CVE-2022-21476	CVE-2022-22827	CVE-2022-0435
CVE-2022-21496	CVE-2022-23852	CVE-2022-0852

Fabricante

Red Hat

Productos afectados

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
Red Hat Gluster Storage Web Administration (for RHEL Server) 3.1 x86_64
Red Hat OpenShift Container Platform 3.11 x86_64
Red Hat OpenShift Container Platform for Power 3.11 ppc64le
Red Hat OpenShift Container Platform 3.10 x86_64
Red Hat OpenShift Container Platform 3.9 x86_64
Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64
Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le
Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.8 for RHEL 8 s390x
Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64

Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.8 for RHEL 8 s390x Red Hat OpenShift Container Platform 4.9 for RHEL 8 x86_64 Red Hat OpenShift Container Platform 4.8 for RHEL 8 x86_64 Red Hat OpenShift Container Platform 4.7 for RHEL 8 x86_64 Red Hat OpenShift Container Platform 4.6 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.9 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for Power 4.8 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for Power 4.7 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for Power 4.6 for RHEL 8 ppc64le Red Hat Gluster Storage Web Administration (for RHEL Server) 3.1 x86_64 Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64 Red Hat Enterprise Linux Server for Power LE – Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux Server for x86_64 – Update Services for SAP Solutions 8.1 x86_64 Convert2RHEL 6 x86_64 Convert2RHEL 7 x86_64
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00624-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00624-01.pdf

CSIRT alerta de vulnerabilidades en sistemas Linux, apodadas «Nimbuspwn»	
Alerta de seguridad cibernética	9VSA22-00625-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2022
Última revisión	28 de abril de 2022
CVE	
CVE-2022-29799 CVE-2022-29800	
Fabricante	
Linux (varias distribuciones)	
Productos afectados	
Varias distribuciones Linux no especificadas por los descubridores de las vulnerabilidades (Microsoft). Algunas de las que han sido a conocer por sus responsables son: Linux Mint Debian Buster 2.0-2 Debian Bullseye 2.1-2 Debian Bookworm 2.1-2 Debian Sid 2.1-2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00625-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00625-01.pdf	

CSIRT alerta de vulnerabilidades en productos Cisco		
Alerta de seguridad cibernética	9VSA22-00626-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	28 de abril de 2022	
Última revisión	28 de abril de 2022	
CVE		
CVE-2022-20746	CVE-2022-20760	CVE-2022-20748
CVE-2022-20751	CVE-2022-20737	CVE-2022-20627
CVE-2022-20757	CVE-2022-20715	CVE-2022-20628
CVE-2022-20743	CVE-2022-20767	CVE-2022-20629
CVE-2022-20759	CVE-2022-20681	CVE-2022-20740
CVE-2022-20742	CVE-2022-20729	CVE-2022-20744
CVE-2022-20745	CVE-2022-20730	
Fabricante		
Cisco		
Productos afectados		
Cisco Firepower Threat Defense Software TCP Proxy. Cisco Firepower Threat Defense Software Snort. Cisco Firepower Threat Defense Software. Cisco Firepower Management Center File Upload. Cisco Adaptive Security Appliance Software Cisco Firepower Threat Defense (FTD) Software. Cisco Adaptive Security Appliance (ASA) Software. Cisco Firepower Management Center (FMC) Software.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00626-01/		
https://www.csirt.gob.cl/media/2022/04/9VSA22-00626-01.pdf		

Actualidad

Ciberconsejos para evitar estafas en redes sociales

Más del 58% de la población del mundo usa redes sociales, según el último estudio de la agencia We Are Social y Hootsuite, gestor de redes sociales, destacando a Facebook, YouTube, WhatsApp, Instagram y Tik Tok como las plataformas más utilizadas.

Lógicamente, esta difusión ha permitido que los delincuentes creen nuevos tipos de estafas a través de las distintas redes sociales. Y para ayudar a que no seamos víctimas de uno de estos fraudes creamos los siguientes consejos, los que también pueden ser descargados aquí: csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-estafas-en-redes-sociales/.

Ciberdiccionario Volumen 3

Para entender los riesgos que acechan en el ciberespacio, como CSIRT de Gobierno compartimos esta semana un tercer volumen de nuestro ciberdiccionario, con definiciones de algunos peligros a los que están expuestas tanto las personas como las instituciones, como asimismo de conceptos muy importantes en nuestra protección frente a estos riesgos.

Pueden descargar el ciberdiccionario también aquí: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-3/

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Maximiliano Zamorano
- Bárbara Palacios
- Juan Alfonso Muñoz Castañeda
- Tomás Eduardo Gaete Fischer
- Víctor Cofré
- Juan Carlos López
- Julio César Cisternas Bascur
- José Alfredo Andaluz Prado
- David Soto
- Mathias Roco
- Gerardo Méndez Ortega
- Marco Antonio Ojeda Vargas
- Carlos
- Elisa Molina H.
- Andrés Aldana F.
- Felipe Alejandro Rosales Jofré
- Paulina Fernanda Alonso Parancán
- Javier Ignacio Gutiérrez Campos