21-05-2020 | Año 1 | N°46

Boletín de Seguridad Cibernética

Semana del 14 al 21 de mayo 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras

Parches

9

para vulnerabilidades

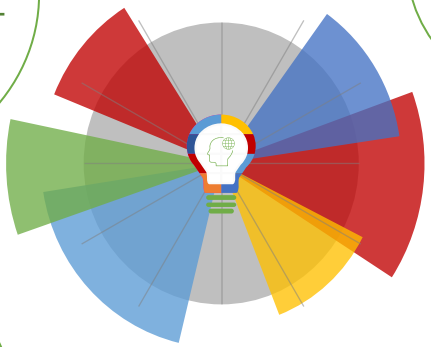
Las mitigaciones son útiles para productos de MongoDb, ClamAV, Moodle, MISP, VMware, Adobe y Google.

Se advirtieron

89

sitios fraudulentos

Asociadas a 29 IP maliciosas



Phishing

11

Campañas

Entre ellos se cuentan phishing bancarios, de servicios de pago y correos corporativos

IPs

155

bloqueadas

Listado de IPs que trataron de realizar escaneos de puertos, DDoS o infectar códigos maliciosos, entre otros.

*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 advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00417-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Mayo de 2020
Última revisión	14 de Mayo de 2020
Indicadores de compromiso	
URL	
scotiabanpersonas[.]cllsp[.]com	
IP	
96[.]9[.]220[.]170	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00417-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00417-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00418-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Mayo de 2020
Última revisión	14 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestadocl[.]sorteoschile[.]com	
IP	
192[.]185[.]214[.]75	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00418-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00418-01.pdf	

Imagen del sitio

CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00419-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
scotiaweb-cl[.]website	
scotiabanckcl[.]com	
IP	
199[.]188[.]200[.]223	
104[.]237[.]2[.]112	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00419-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00419-01.pdf	

Imagen del sitio

CSIRT informa sobre un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00420-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Mayo de 2020
Última revisión	07 de Mayo de 2020
Indicadores de compromiso	
URL	
seguro.cl-bestado[.]com	
IP	
199[.]188[.]200[.]216	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00420-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00420-01.pdf	

Imagen del sitio

CSIRT advierte de 3 sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00421-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Mayo de 2020
Última revisión	16 de Mayo de 2020
Indicadores de compromiso	
URL	
estadocl[.]sorteoschile[.]com	
htlps-wwv-bancoestado-cl[.]clinicadentistaruclf[.]com/personas-cl	
bancoestado[.]sorteoschile[.]com	
IP	
95[.]111[.]244[.]218	
162[.]241[.]2[.]177	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00421-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00421-01.pdf	

Imagen del sitio

CSIRT advierte de dos dominios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00422-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Mayo de 2020
Última revisión	16 de Mayo de 2020
Indicadores de compromiso	
URL	
bancodechilepersonax[.]vapehousebh[.]com	
bancodechilepersonax[.]ezzgroup-eg[.]com	
IP	
69[.]174[.]53[.]205	
96[.]127[.]128[.]202	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00422-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00422-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00423-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
Indicadores de compromiso	
URL	
scotiachile[.]cl-support[.]login[.]recruitmentagency[.]net/scoticheyo2020/IONO2X/login/CJODP/personas//	
IP	
130[.]193[.]89[.]178	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00423-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00423-01.pdf	

Imagen del sitio

CSIRT advierte de cuatro portales bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00424-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
Indicadores de compromiso	
URL	
bancapersonabancoestado[.]site	
bancorstado[.]cl	
bancoestao[.]cl	
bancostado[.]cl	
IP	
185[.]61[.]153[.]111	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00424-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00424-01.pdf	

Imagen del sitio

CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00425-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2020
Última revisión	20 de mayo de 2020
Indicadores de compromiso	
URL	
bancochile.cl[.]bouph[.]com	
bchile[.]mcblack1[.]com	
IP	
142[.]11[.]253[.]177	
213[.]108[.]242[.]100	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00425-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00425-01.pdf	

Phishing

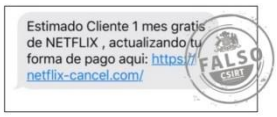
Imagen del mensaje

CSIRT advierte phishing bancario con opción de pago por covid-19	
Alerta de seguridad cibernética	8FPH20-00214-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://pneussantahelena.com[.]br/wp-content/cencosud.php	
hxxps://tarjetacencosud-chile-activa[.]ga/	
IP	
[103.248.146.100]	
[103.248.146.2]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00214-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00214-01.pdf	

Imagen del mensaje

CSIRT advierte campaña de phishing por falso bono covid-19	
Alerta de seguridad cibernética	8FPH20-00215-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
https[:]//ayudas-chile[.]blogspot[.]com/	
10[.]the31news[.]com, 15[.]the31news[.]com, 19[.]the31news[.]com, 20[.]the31news[.]com, 21[.]the31news[.]com, 23[.]the31news[.]com, 24[.]the31news[.]com, 25[.]the31news[.]com, 29[.]the31news[.]com, 30[.]the31news[.]com, 31[.]the31news[.]com, 33[.]the31news[.]com, 35[.]the31news[.]com, 36[.]the31news[.]com, 37[.]the31news[.]com, 40[.]the31news[.]com, 41[.]the31news[.]com, 46[.]the31news[.]com, 48[.]the31news[.]com, 49[.]the31news[.]com, 5[.]the31news[.]com, 50[.]the31news[.]com, 51[.]the31news[.]com, 53[.]the31news[.]com, 54[.]the31news[.]com, 57[.]the31news[.]com, 58[.]the31news[.]com, 59[.]the31news[.]com, 6[.]the31news[.]com, 60[.]the31news[.]com, 61[.]the31news[.]com, 63[.]the31news[.]com, 65[.]the31news[.]com, 7[.]the31news[.]com, 70[.]the31news[.]com, 71[.]the31news[.]com, 72[.]the31news[.]com, 74[.]the31news[.]com, 78[.]the31news[.]com, 79[.]the31news[.]com, 81[.]the31news[.]com, 83[.]the31news[.]com, 85[.]the31news[.]com, 88[.]the31news[.]com, 92[.]the31news[.]com, 93[.]the31news[.]com, 96[.]the31news[.]com, 97[.]the31news[.]com, 98[.]the31news[.]com	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00215-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00215-01.pdf	

Imagen del mensaje



CSIRT advierte de smishing por pago en servicio streaming	
Alerta de seguridad cibernética	8FPH20-00216-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
https[:]//netflix-cancel[.]com/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00216-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00216-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing bancario de crédito pre-aprobado	
Alerta de seguridad cibernética	8FPH20-00217-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://pneussantahelena[.]com.br/docs/ripley.php	
hxxps://miportal-banco-ripley-cl[.]cf/	
IP	
[103.248.146.100]	
[103.248.146.2]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00217-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00217-01.pdf	

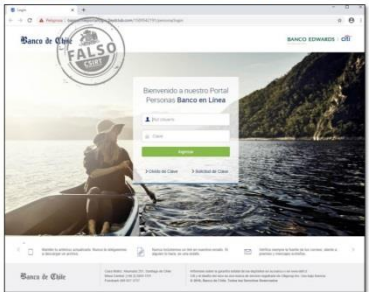
Imagen del mensaje

CSIRT advierte de phishing por depósito de pensiones	
Alerta de seguridad cibernética	8FPH20-00218-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/35XKEDO?l=www.bancoestado.cl	
hxxp://teraon[.]ru/engl/enviar.php?l=493041686	
hxxp://www.piotrlicznerski[.]pl/activacion/cuenta-ehkt/	
https://roisport.co[.]il/Avisos/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[5.45.117.11]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00218-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00218-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por caducidad de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00219-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp://asesorehs.com[.]pe/es/	
hxxp://bancoestado3.tonohost[.]com/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[212.227.20.174]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00219-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00219-01.pdf	

Imagen del sitio



CSIRT advierte de phishing bancario por sincronización de digipass	
Alerta de seguridad cibernética	8FPH20-00220-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://bancochileportallogin.2mdclub[.]com/1589542191/persona/login	
IP	
[45.147.228.99]	
[45.147.228.83]	
Otros IOCs del informe:	
2 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00220-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00220-01.pdf	

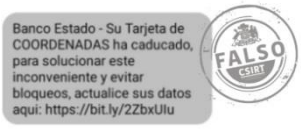
Imagen del mensaje

CSIRT advierte estafa que involucra encomienda internacional con multa	
Alerta de seguridad cibernética	8FPH20-00221-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Mayo de 2020
Última revisión	16 de Mayo de 2020
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00220-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00220-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por entrega de bono covid-19	
Alerta de seguridad cibernética	8FPH20-00222-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Mayo de 2020
Última revisión	16 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp://consticaous[.]site/activala/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[170.239.85.226]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00222-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00222-01.pdf	

Imagen del mensaje

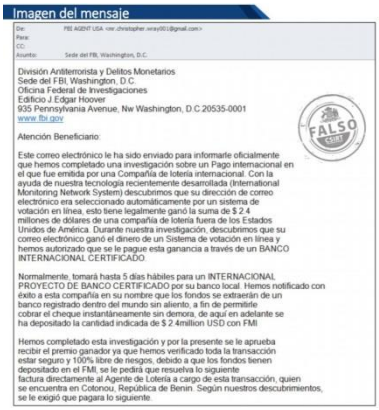


CSIRT advierte Smishing por vencimiento de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00223-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Mayo de 2020
Última revisión	18 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp[:]//bit[.]ly/2ZbxUIu	
hxxps[:]//app.movichilestad-smsch[.]com/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00223-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00222-01.pdf	

Imagen del mensaje

CSIRT advierte phishing por falsa entrega de bono covid-19	
Alerta de seguridad cibernética	8FPH20-00224-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Mayo de 2020
Última revisión	18 de Mayo de 2020
Indicadores de compromiso	
URL	
Hxxps[:]//bit[.]ly/3dCUUnF?l=www.bancoestado.cl	
Hxxp[:]//teraon[.]ru/engl/enviar.php?l=1104867473	
Hxxps[:]//creamcheese[.]uy/_personas/www.bancoestado.cl/	
IP	
[103.227.177.43]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00224-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00224-01.pdf	

Imagen del mensaje



CSIRT advierte phishing por premio de lotería internacional	
Alerta de seguridad cibernética	8FPH20-00225-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Mayo de 2020
Última revisión	18 de Mayo de 2020
Indicadores de compromiso	
IP	
[74.6.134.41]	
[74.6.130.40]	
[74.6.133.40]	
[74.6.133.123]	
[74.6.134.125]	
[209.85.160.196]	
Otros IOCs del informe:	
2 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00225-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00225-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por mantención de servicios bancarios	
Alerta de seguridad cibernética	8FPH20-00226-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp://rakitys[.]info/natu/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.121.8]	
[45.7.231.109]	
Otros IOCs del informe:	
2 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00226-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00226-01.pdf	

Malware

CSIRT informa sobre tres variantes de malware activos	
Alerta de seguridad cibernética	2CMV20-00062-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
Indicadores de compromiso	
Otros IOCs del informe:	
3 variantes de Hash	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00062-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00062-01.pdf	

CSIRT advierte campaña de phishing con malware por bono de combustible	
Alerta de seguridad cibernética	2CMV20-00063-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Mayo de 2020
Última revisión	18 de Mayo de 2020
Indicadores de compromiso	
URL	
Hxxps[:]//combustible[.]gratis/shell/share.html#	
Hxxps[:]//the-best-apps[.]net/?m=1I9SMAINSTREAM&a=1589819154mb25098862078	
Hxxp[:]//mobileoffers[.]info/?off=1	
Hxxps[:]//4444063.catchtheclick[.]com	
Hxp[:]//ads.trisier[.]com/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00061-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00061-01.pdf	

CSIRT advierte de malware en correo sobre investigación policial	
Alerta de seguridad cibernética	2CMV20-00064-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo de 2020
Indicadores de compromiso	
DNS	
atiku2[.]duckdns[.]org	
IP	
185[.]165[.]153[.]28	
3 tipos de Hash	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00064-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00064-01.pdf	

CSIRT advierte de malware en correo sobre investigación policial	
Alerta de seguridad cibernética	2CMV20-00065-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo de 2020
Indicadores de compromiso	
IP	
172[.]111[.]188[.]199	
3 tipos de Hash	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00065-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00065-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones de FreeBSD para su Sistema Operativo	
Alerta de seguridad cibernética	9VSA-00213-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
CVE	
CVE-2020-15878, CVE-2020-15879, CVE-2020-15880	
Fabricante	
FreeBSD	
Producto afectado	
FreeBSD versión 11.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00213-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00213-01.pdf	

CSIRT comparte actualizaciones de MongoDB para base de datos	
Alerta de seguridad cibernética	9VSA20-00214-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
CVE	
CVE-2020-7921	
Fabricante	
MongoDB	
Producto afectado	
MongoDB Server Todas las versiones anteriores a la 4.3.3., todas las versiones anteriores a la 4.2.3., todas las versiones anteriores a la 4.0.15., y todas las versiones anteriores a la 3.6.18.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00214-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00214-01.pdf	

CSIRT comparte actualizaciones de ClamAV para su AntiVirus	
Alerta de seguridad cibernética	9VSA20-00215-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Mayo de 2020
Última revisión	15 de Mayo de 2020
CVE	
CVE-2020-3341, CVE-2020-3327	
Fabricante	
ClamAV	
Producto afectado	
ClamAV versión 0.102.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00215-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00215-01.pdf	

CSIRT comparte actualizaciones liberadas por Moodle	
Alerta de seguridad cibernética	9VSA20-00216-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Mayo de 2020
Última revisión	19 de Mayo de 2020
CVE	
CVE-2020-10738, CVE-2018-1999024	
Fabricante	
Moodle	
Producto afectado	
Moodle versiones 3.8 hasta la 3.8.2, 3.7 hasta la 3.7.5, 3.6 hasta la 3.6.9, 3.5 hasta la 3.5.11 y versiones anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00216-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00216-01.pdf	

CSIRT comparte actualizaciones para MISP	
Alerta de seguridad cibernética	9VSA20-00217-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
CVE	
CVE-2020-13153	
Fabricante	
MISP	
Producto afectado	
Esta vulnerabilidad afecta a todas las versiones de MISP.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00217-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00217-01.pdf	

CSIRT comparte actualizaciones liberados por Google	
Alerta de seguridad cibernética	9VSA20-00218-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
CVE	
CVE-2020-6465, CVE-2020-6466, CVE-2020-6467, CVE-2020-6468, CVE-2020-6469, CVE-2020-6470, CVE-2020-6471, CVE-2020-6472 CVE-2020-6473, CVE-2020-6474, CVE-2020-6475, CVE-2020-6476 CVE-2020-6477, CVE-2020-6478, CVE-2020-6479, CVE-2020-6480 CVE-2020-6481, CVE-2020-6482, CVE-2020-6483, CVE-2020-6484 CVE-2020-6485, CVE-2020-6486, CVE-2020-6487, CVE-2020-6488 CVE-2020-6489, CVE-2020-6490, CVE-2020-6491	
Fabricante	
Google	
Producto afectado	
Google Chrome desde la versión 83.0.4103.0 hasta la 83.0.4103.60.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00218-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00218-01.pdf	

CSIRT comparte actualizaciones liberadas por Adobe	
Alerta de seguridad cibernética	9VSA20-00219-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
CVE	
CVE-2020-9592, CVE-2020-9593, CVE-2020-9594, CVE-2020-9595 CVE-2020-9596, CVE-2020-9597, CVE-2020-9598, CVE-2020-9599 CVE-2020-9600, CVE-2020-9601, CVE-2020-9602, CVE-2020-9603 CVE-2020-9604, CVE-2020-9605, CVE-2020-9606, CVE-2020-9607 CVE-2020-9608, CVE-2020-9609, CVE-2020-9610, CVE-2020-9611 CVE-2020-9612, CVE-2020-9613, CVE-2020-9614, CVE-2020-9615	
Fabricante	
Adobe	
Producto afectado	
Acrobat DC versión 2020.006.20042 y anteriores., Acrobat Reader DC versión 2020.006.20042 y anteriores., Acrobat 2017 versión 2017.011.30166 y anteriores., Acrobat Reader 2017 versión 2017.011.30166 y anteriores., Acrobat 2015 2015.006.30518 y anteriores., Acrobat Reader 2015 versión 2015.006.30518 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00219-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00219-01.pdf	

CSIRT comparte actualizaciones liberadas por VMware	
Alerta de seguridad cibernética	9VSA20-00220-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
CVE	
CVE-2020-3956	
Fabricante	
VMware	
Producto afectado	
vCloud Director versiones 9.1.x para Linux y 9.5.x, 9.7.x y 10.0.x para Linux y PhotonOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00220-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00220-01.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad:

IoC	Motivo	IoC	Motivo
23.248.188.94	Port Scan	103.57.190.92	Port Scan
192.210.139.177	Port Scan	178.62.60.233	Port Scan
103.145.12.95	Port Scan	64.227.110.18	Port Scan
45.143.220.5	Port Scan	42.115.18.166	Port Scan
94.102.51.58	Port Scan	195.154.184.170	Port Scan
187.250.59.183	Malware	176.57.138.47	Port Scan
201.127.103.93	Malware	162.243.136.88	Port Scan
68.60.221.169	Malware	159.65.152.232	Port Scan
86.233.4.153	Malware	159.89.85.202	Port Scan
86.123.106.54	Malware	89.248.162.247	Port Scan
198.71.233.227	Malware	134.209.155.5	Port Scan
60.190.248.11	Hacking	216.144.248.186	Port Scan
144.217.34.153	Port Scan	162.243.136.81	Port Scan
205.185.118.183	Port Scan	162.243.136.243	Port Scan
157.52.193.79	Port Scan	162.243.136.20	Port Scan
209.126.1.2	Port Scan	162.243.136.91	Port Scan
213.233.179.200	Port Scan	198.50.231.216	Port Scan
162.243.136.232	Port Scan	142.93.208.158	Port Scan
205.185.123.126	Port Scan	162.243.136.141	Port Scan
190.187.120.49	Port Scan	158.69.30.91	Port Scan
107.189.11.56	Port Scan	14.143.251.38	Malware
77.247.109.95	Port Scan	45.233.169.6	Malware
195.154.189.8	Port Scan	138.59.143.222	Malware
51.159.59.122	Port Scan	193.254.245.178	Port Scan
167.172.201.148	DDoS	185.153.180.27	Port Scan
185.132.53.133	Port Scan	185.53.88.229	Port Scan
51.77.133.28	Port Scan	162.243.136.201	Port Scan
94.102.51.58	Port Scan	62.210.86.131	Port Scan
103.145.12.77	Port Scan	167.172.104.27	Port Scan
104.129.4.186	Port Scan	51.83.216.198	Port Scan

51.159.64.153	Port Scan	193.19.175.163	Port Scan
51.161.68.189	Port Scan	45.143.220.122	Port Scan
138.197.12.187	Port Scan	46.105.117.221	Port Scan
134.122.79.129	Port Scan	93.99.104.205	Hacking
103.130.112.110	Port Scan	93.99.104.101	Port Scan
103.15.141.126	Port Scan	89.188.72.112	Port Scan
110.137.70.211	Port Scan	178.62.55.70	Port Scan
159.65.245.197	Port Scan	158.69.1.201	Port Scan
137.74.155.171	Port Scan	45.125.65.46	Port Scan
139.99.48.185	Port Scan	74.91.125.219	Port Scan
213.202.225.47	Port Scan	51.83.216.198	Port Scan
51.159.0.163	Port Scan	51.83.216.198	Port Scan
162.243.136.203	Port Scan	51.83.216.197	Port Scan
51.158.77.33	Port Scan	88.80.148.230	Port Scan
45.148.10.22	Port Scan	201.184.37.83	Port Scan
139.99.2.155	Port Scan	93.174.89.55	Port Scan
188.255.217.242	Port Scan	51.15.237.225	Port Scan
149.202.87.6	Port Scan	162.243.136.95	Port Scan
31.186.250.229	Port Scan	85.217.205.129	Port Scan
138.197.73.177	Port Scan	162.241.50.117	Port Scan
36.78.202.178	Port Scan	92.38.171.36	Port Scan
82.102.173.87	Port Scan	156.96.117.40	Port Scan
185.39.11.187	Port Scan	92.38.171.36	Port Scan
118.70.113.2	Port Scan	193.70.60.85	Port Scan
46.101.6.56	Port Scan	61.255.239.24	Port Scan
45.143.223.245	Port Scan	139.99.149.9	Port Scan
45.154.1.102	Port Scan	92.38.171.36	Port Scan
162.243.136.8	Port Scan	193.70.60.85	Port Scan
162.243.136.156	Port Scan	165.22.84.195	Port Scan
185.143.75.74	Port Scan	128.199.232.80	Port Scan
162.243.136.189	Port Scan	162.243.136.52	Port Scan
62.171.188.97	Port Scan	45.148.10.72	Port Scan
163.172.210.152	Port Scan	220.135.206.63	Port Scan
185.53.88.226	Port Scan	162.243.136.42	Port Scan
102.129.224.62	Port Scan	45.79.189.105	DDoS
80.211.241.202	Port Scan	185.142.236.35	DDoS
159.89.94.13	Port Scan	90.226.80.9	DDoS
1.1.156.106	Port Scan	94.69.235.128	DDoS

162.243.136.249	Port Scan	170.106.36.31	DDoS
159.89.147.102	Port Scan	54.36.149.15	DDoS
182.53.103.199	Port Scan	124.156.210.20	DDoS
144.217.255.187	Port Scan	185.173.35.61	DDoS
37.49.230.128	Port Scan	185.153.196.245	Port Scan
185.153.197.11	Port Scan	45.143.220.6	Port Scan
198.98.51.63	Port Scan	103.145.12.122	Port Scan
118.160.101.77	Port Scan	198.98.51.63	Port Scan
5.182.210.95	Port Scan	185.153.197.11	Port Scan
95.111.240.249	Port Scan		

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.

Investigación

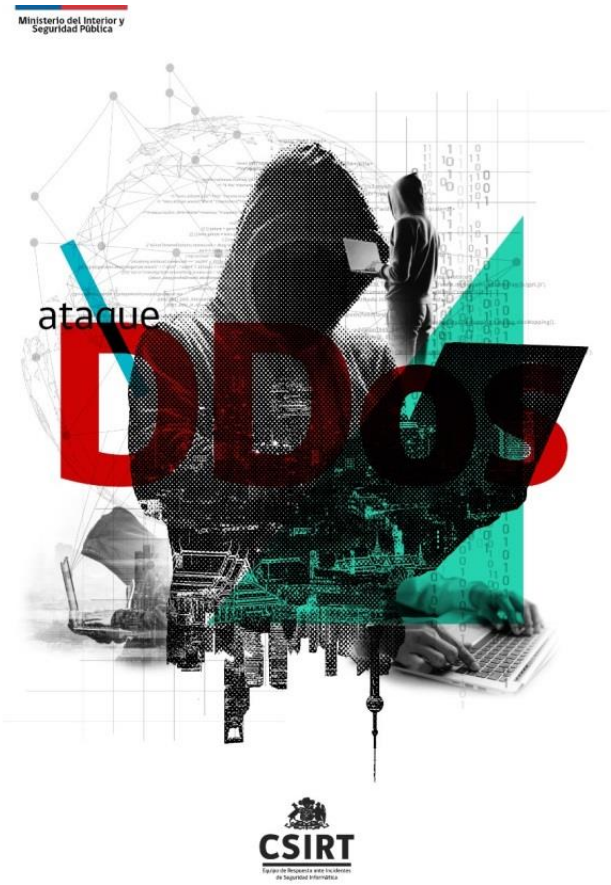
Ataque de DoS y DDos

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, presentó la edición número 4 de análisis de amenazas cibernéticas, que la reciente semana abordó los **Ataques de DoS y DDos**, artículo que fue elaborado por Carlos Silva Caffi, analista de nivel 2 de CSIRT.

La investigación tratade uno de los ataques más comunes que amenazan la seguridad cibernética de las instituciones, el que **puede afectar seriamente la disponibilidad de actividades comerciales, trámites bancarios o la entrega de servicios públicos**, por ejemplo.

En este artículo se explica la estructura del ataque, la motivación de los atacantes para ejecutarlo, cuales son las diferencias entre DoS y DDoS, y algunos de los tipos de ataques.

El análisis utiliza como **referencia de análisis el modelo OSI** que describe la conectividad de red, permitiendo identificar a las capas de red, transporte, presentación y aplicación como aquellas donde se concentran los ataques.



Ver en: https://www.csirt.gob.cl/reportes/an2-2020-04/

Manual de procedimiento de revocación de nombre de dominio

Conscientes del aumento de registros de dominios fraudulentos y preocupados por mantener un ecosistema ciberseguro, el CSIRT de Gobierno elaboró **este manual de procedimiento de revocación de nombre de dominio** para guiar a quienes deberán enfrentarse a este tipo de situaciones apoyados con el software "La Campana".

En la primera parte, se aborda brevemente la finalidad de la guía, como complemento al uso del software "La Campana". La segunda sección introduce al lector en cuestiones relativas a la administración, conflictos generados a partir de los nombres de dominio. En el tercer apartado, el manual describe cada paso del procedimiento desde la presentación del conflicto, la forma de realizar la revocación y cómo se debe llevar a cabo esto en el sitio de Nic Chile. Posteriormente, se analizan los tipos de revocación posibles y cuando proceden, entre otros. Finalmente, se abordan las malas prácticas en la inscripción de nombres de dominio, la ciberocupación o uso del nombre con mala fe y el secuestro inverso de los nombres de dominio.

Ver en: https://www.csirt.gob.cl/reportes/manual-de-dominio/

Actualidad

Esta semana celebramos el día internacional de la internet y CSIRT conmemoró la oportunidad publicando un breve resumen de su historia.

Hitos de la historia de Internet

El 17 de mayo se celebró el Día Mundial de Internet. Para muchos quizás su historia es desconocida, por eso les contamos hitos interesantes de cómo nació y su evolución.

¿Por qué nace Internet?

Surgió en Estados Unidos como un proyecto militar, en un contexto de posibles ataques hacia ese país, por lo que el objetivo era asegurar las comunicaciones desde diferentes puntos del país, en un contexto de posibles ataques

La noticia completa está disponible en el siguiente enlace: https://www.csirt.gob.cl/noticias/hitos-de-la-historia-de-internet/

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 del mismo.

- Dionny Contreras.
  Twitter: @Dionnycontreras
- Bernardo Avilés
- Romel Rivas:
  Linkedin:
  https://www.linkedin.com/in/romelrivas/
- Rodrigo Cortés

CSIRT Gobierno de Chile | Firmado digitalmente por CSIRT Gobierno de Chile Fecha: 2020.05.22 19:53:36 -04'00'