

25-06-2020
N°51

edición
ANIVERSARIO

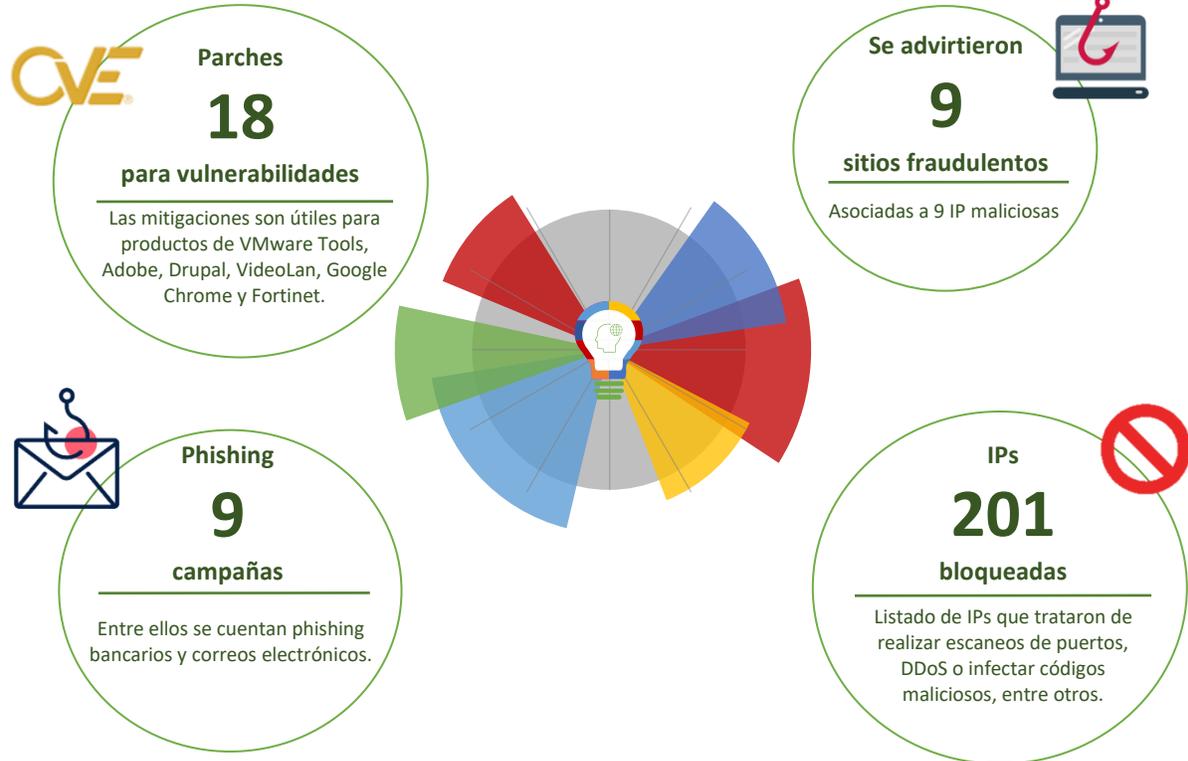


Boletín de Seguridad Cibernética

Semana del 18 al 24 de junio 2020



Resumen de la semana en cifras



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

Contenido

Sitios fraudulentos.....	3
Phishing.....	8
Vulnerabilidades.....	13
Indicadores de Compromisos.....	16
Recomendaciones y Buenas Prácticas.....	19
Actualidad.....	20
Investigación.....	22
Muro de la Fama.....	23
Resumen anual.....	24
Indicadores generales.....	25
URL informadas por semana.....	26
IP informadas por semana.....	27
Vulnerabilidades por semana.....	28
Investigaciones.....	29
Concientización.....	30
Muro de la fama 2019-2020.....	31

Sitios fraudulentos

Imagen del sitio



CSIRT advierte de portal bancario fraudulento

Alerta de seguridad cibernética	8FFR20-00452-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Junio de 2020
Última revisión	17 de Junio de 2020
Indicadores de compromiso	
URL	http[:]//banco-estado[.]credit/1592359985/imagenes/comun2008/banca-en-linea-personas[.]html
IP	85.187.132.169
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr20-00452-01/
	https://www.csirt.gob.cl/media/2020/06/8FFR20-00452-01.pdf

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento

Alerta de seguridad cibernética	8FFR20-00453-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
Indicadores de compromiso	
URL	http[:]//bancoestador[.]com/1592530439/imagenes/comun2008/banca-en-linea-personas[.]html
IP	185.61.154.34
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr20-00453-01/
	https://www.csirt.gob.cl/media/2020/06/8FFR20-00453-01.pdf

Imagen del sitio



CSIRT advierte de sitio de streaming fraudulento

Alerta de seguridad cibernética	8FFR20-00454-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
Indicadores de compromiso	
URL	http[:]//ts-netflix[.]com/
IP	162.0.229.69
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00454-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00454-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de pagos en línea fraudulento

Alerta de seguridad cibernética	8FFR20-00455-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Junio de 2020
Última revisión	22 de Junio de 2020
Indicadores de compromiso	
URL	http[:]//paypalgb[.]com/
IP	184.168.221.66
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00455-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00455-01.pdf	



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00456-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://sinatexcom[.]ir/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html
IP	158.58.186.50
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00456-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00456-01.pdf	



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00457-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://192.119.70[.]33/imagenes/comun2008/login.php
IP	192.119.70.33
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00457-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00457-01.pdf	

Imagen del sitio



CSIRT advierte un sitio bancario fraudulento

Alerta de seguridad cibernética	8FFR20-00458-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020

Indicadores de compromiso

URL
[https://dplwood\[.\]com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas\[.\]html](https://dplwood[.]com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html)

IP
 31.131.22.61

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr20-00458-01/>
<https://www.csirt.gob.cl/media/2020/06/8FFR20-00458-01.pdf>

Imagen del sitio



CSIRT advierte sitio fraudulento de cadena de supermercado

Alerta de seguridad cibernética	8FFR20-00459-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020

Indicadores de compromiso

URL
[http://cupon-lider\[.\]com/#](http://cupon-lider[.]com/#)

IP
 45.148.120.2

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr20-00459-01/>
<https://www.csirt.gob.cl/media/2020/06/8FFR20-00459-01.pdf>



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00460-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020
Indicadores de compromiso	
URL	https://skmc[.]in/Avisos/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html
IP	199.79.62.196
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr20-00460-01/
	https://www.csirt.gob.cl/media/2020/06/8FFR20-00460-01.pdf

Phishing

Imagen del mensaje



CSIRT advierte phishing bancario por inconveniente en dispositivo	
Alerta de seguridad cibernética	8FPH20-00247-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Junio de 2020
Última revisión	18 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://casamae.com[.]br/b1cc9410c9d1b8bb567478dc313e00db hxxps://zingy-bingo[.]com/1592520245/login/personas
IP	[185.5.55.38]
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00247-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00247-01.pdf	

Imagen del mensaje



CSIRT advierte phishing con falso cupón de supermercado	
Alerta de seguridad cibernética	8FPH20-00248-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://superma[.]co/Lider hxxps://junebox[.]live/markets/es/lider/ hxxps://bonxmedia[.]com/subscriptions/checkoutaff/panther-direct-3X
IP	5.188.9.150
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00248-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00248-01.pdf	

Imagen del mensaje



CSIRT advierte de Smishing por falso bono de emergencia	
Alerta de seguridad cibernética	8FPH20-00249-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/2N2C4eb	
hxxp://192.119.68[.]238/bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00249-01/	
https://www.csirt.gob.cl/media/2020/06/8FPH20-00249-01.pdf	

Imagen del mensaje



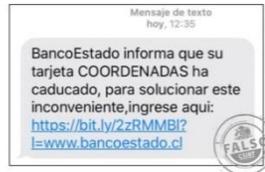
CSIRT advierte phishing bancario por suspensión de cuenta	
Alerta de seguridad cibernética	8FPH20-00250-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	hxxps://jayashaki[.]com/18fb865a3096b2064242b292549cd44c https://canaldigitalscotienlinea[.]com/1592924516/login/personas
IP	[212.24.105.73]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00250-01/ https://www.csirt.gob.cl/media/2020/06/8FPH20-00250-01.pdf

Imagen del mensaje



CSIRT advierte phishing por problema en cuenta de servicio de software	
Alerta de seguridad cibernética	8FPH20-00251-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	hxxps://limiteced.access.akojagia[.]com/account/?view=login&appIdKey=53bdcc7a4a47bd9&country=CL
IP	162.241.117.207
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00251-01/ https://www.csirt.gob.cl/media/2020/06/8FPH20-00251-01.pdf

Imagen del mensaje



CSIRT advierte smishing por caducidad de tarjeta de coordenadas	
Alerta de seguridad cibernética	8FPH20-00252-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://bit[.]ly/2zRMMBI?l=www[.]bancoestado[.]cl
	hxxp://wendytherapy[.]com/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html#
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00252-01/
	https://www.csirt.gob.cl/media/2020/06/8FPH20-00252-01.pdf

Imagen del mensaje



CSIRT advierte Smishing bancario por bloqueo de acceso a cuenta	
Alerta de seguridad cibernética	8FPH20-00253-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://bit[.]ly/www-BancoEstado
	http://192.119.71.107/
	hxxp://142.11.236.23/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00253-01/
	https://www.csirt.gob.cl/media/2020/06/8FPH20-00253-01.pdf

Imagen del sitio



CSIRT advierte de phishing de supermercado vía WhatsApp

Alerta de seguridad cibernética	8FPH20-00254-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020
Indicadores de compromiso	
URL	hxxp://cupon-lider[.]com
	hxxps://junebox[.]me/markets/es/lider/
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00254-01/
	https://www.csirt.gob.cl/media/2020/06/8FPH20-00254-01.pdf

Imagen del mensaje



CSIRT advierte phishing por problema en DigiPass

Alerta de seguridad cibernética	8FPH20-00255-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020
Indicadores de compromiso	
URL	https://bancoenlinea.bchile-alerta.com
	hxxps://homepersonas.lineaportal-cl[.]com/
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph20-00255-01/
	https://www.csirt.gob.cl/media/2020/06/8FPH20-00255-01.pdf

Vulnerabilidades



CSIRT advierte vulnerabilidades en Gestor de Cotenidos de Drupal	
Alerta de seguridad cibernética	9VSA20-00247-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
CVE	
CVE-2020-13663 - CVE-2020-13664 - CVE-2020-13665	
Fabricante	
Drupal	
Producto afectado	
Drupal versiones 7.x, 8.x y 9.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00247-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00247-01.pdf	



CSIRT advierte vulnerabilidades en VLC obtenidas de VideoLan	
Alerta de seguridad cibernética	9VSA20-00248-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Junio de 2020
Última revisión	19 de Junio de 2020
CVE	
CVE-2020-9308 - CVE-2020-13428 - CVE-2019-19221	
Fabricante	
VideoLan	
Productos afectados	
Afecta a todas las versiones del reproductor VLC.	
Afecta a todas las versiones del reproductor VLC para macOS o iOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00248-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00248-01.docx.pdf	



CSIRT advierte vulnerabilidad y comparte mitigación para VMwarweTools

Alerta de seguridad cibernética	9VSA20-00249-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Junio de 2020
Última revisión	12 de Junio de 2020

CVE

CVE-2020-3972

Fabricante

VMware Tools

Producto afectado

VMware Tools versión 11.x.x y anteriores para macOS.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00249-01/>

<https://www.csirt.gob.cl/media/2020/06/9VSA20-00249-01.pdf>



CSIRT advierte vulnerabilidades y comparte mitigaciones liberadas por Google para Chrome

Alerta de seguridad cibernética	9VSA20-00250-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020

CVE

CVE-2020-6509 - CWE-20

Fabricante

Google Chrome

Producto afectado

Google Chrome desde la versión 83.0.4103.0 hasta la 83.0.4103.115.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00250-01/>

<https://www.csirt.gob.cl/media/2020/06/9VSA20-00250-01.pdf>



CSIRT advierte 3 vulnerabilidades y comparte mitigaciones liberadas por Adobe para AdobeFrameMaker

Alerta de seguridad cibernética	9VSA20-00251-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020

CVE

CVE-2020-9636 - CVE-2020-9634 - CVE-2020-9635

Fabricante

Adobe

Producto afectado

Adobe FrameMaker versión 2019.0.5 y anteriores para Windows.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00251-01/>

<https://www.csirt.gob.cl/media/2020/06/9VSA20-00251-01.pdf>



CSIRT advierte vulnerabilidades y mitigaciones obtenidas de FortiNet

Alerta de seguridad cibernética	9VSA20-00252-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio de 2020

CVE

CVE-2019-6693 - CVE-2020-9289 - CVE-2020-9288

CVE-2015-0279 - CVE-2020-6644 - FG-IR-20-036

Fabricante

FortiNet

Productos afectados

FortiOS versión 6.2.0, desde la 6.0.0 hasta la 6.0.6, y 5.6.10 y anteriores. (Afecta a todos los datos de credenciales de tipo «ENC» en la configuración de FortiOS CLI, excepto a la clave del administrador).

FortiManager versión 6.2.3 y anteriores.

FortiWLC versión 8.5.1 y anteriores.

FortiSIEM versión 5.2.8 y anteriores.

FortiDeceptor versión 3.0.0 y anteriores.

FortiAnalyzer versión 6.4.0, 6.2.3 y anteriores*.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00252-01/>

<https://www.csirt.gob.cl/media/2020/06/9VSA20-00252-01.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 escaneos 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
144.91.117.70	Port Scan	183.207.113.106	Port Scan
45.148.10.97	Port Scan	183.207.113.107	Port Scan
45.143.220.243	Port Scan	62.24.181.212	Port Scan
77.247.110.101	Port Scan	62.24.181.213	Port Scan
84.247.197.248	Port Scan	192.87.30.48	Port Scan
5.230.69.6	Port Scan	217.21.193.74	Port Scan
176.58.103.126	Port Scan	71.6.231.186	Port Scan
66.113.184.33	Port Scan	129.250.206.86	Port Scan
5.188.168.36	Malware	216.244.66.203	Port Scan
114.79.134.129	Malware	74.82.47.12	Port Scan
139.5.237.27	Malware	74.82.47.30	Port Scan
51.83.134.142	Hacking	222.186.61.19	Port Scan
167.71.36.101	Port Scan	124.156.54.68	Port Scan
79.124.62.250	Port Scan	144.217.77.27	Port Scan
199.127.62.158	Port Scan	37.49.229.182	Port Scan
103.145.12.182	Port Scan	51.255.109.171	Port Scan
2.56.176.162	Port Scan	78.128.113.116	Port Scan
185.53.88.240	Port Scan	80.86.226.130	Port Scan
192.241.192.66	Port Scan	178.238.79.196	Port Scan
194.26.29.154	Port Scan	212.42.122.66	Port Scan
194.26.29.109	Port Scan	206.81.7.1	Port Scan
194.26.29.250	Port Scan	128.14.181.170	Port Scan
194.26.25.10	Port Scan	45.95.168.202	Port Scan
185.153.196.5	Port Scan	107.189.11.149	Port Scan
64.225.20.69	Port Scan	107.191.102.88	Port Scan
157.52.193.122	Port Scan	193.142.146.224	Port Scan
172.83.43.131	Hacking	103.145.12.177	Port Scan
185.220.101.1	Port Scan	192.241.211.98	Port Scan
185.220.101.193	Port Scan	185.132.53.239	Port Scan
94.102.56.215	Port Scan	89.248.160.167	Port Scan

176.10.99.200	Port Scan	185.153.180.38	Port Scan
146.88.240.4	Port Scan	185.103.110.146	Port Scan
63.183.191.26	Port Scan	94.102.56.130	Port Scan
117.34.127.41	Port Scan	185.200.118.86	Port Scan
64.225.102.53	Port Scan	192.241.229.64	Port Scan
181.49.247.206	Malware	192.241.219.95	Port Scan
159.89.163.240	Port Scan	212.70.149.82	Port Scan
54.39.163.178	Port Scan	212.70.149.50	Port Scan
46.101.46.78	Port Scan	212.70.149.2	Port Scan
45.143.220.116	Port Scan	212.70.149.18	Port Scan
185.200.118.57	Port Scan	185.143.75.153	Port Scan
139.99.124.31	Port Scan	185.143.72.25	Port Scan
107.158.144.66	Port Scan	185.143.72.34	Port Scan
157.230.8.174	Port Scan	78.128.113.108	Port Scan
51.79.149.123	Port Scan	185.143.72.16	Port Scan
45.143.220.133	Port Scan	141.98.80.150	Port Scan
194.26.29.215	Port Scan	185.234.218.195	Port Scan
194.26.25.11	Port Scan	185.234.218.82	Port Scan
163.172.199.18	Port Scan	151.80.237.223	Port Scan
64.225.106.116	Port Scan	178.32.144.164	Port Scan
94.215.156.178	Port Scan	37.59.160.147	Port Scan
159.89.54.108	Port Scan	37.49.224.249	Port Scan
195.54.160.135	Port Scan	192.241.211.155	Port Scan
195.54.160.135	Hacking	192.241.214.50	Port Scan
139.99.112.172	Port Scan	192.241.216.162	Port Scan
194.26.29.249	Port Scan	192.241.211.169	Port Scan
194.26.29.9	Port Scan	192.241.214.158	Port Scan
185.39.9.150	Port Scan	206.212.248.178	Malware
45.143.220.174	Port Scan	192.241.227.73	Port Scan
144.217.76.62	Port Scan	192.241.214.233	Port Scan
167.99.60.170	Port Scan	192.241.214.90	Port Scan
89.248.168.220	Port Scan	192.241.224.91	Port Scan
51.254.104.180	Port Scan	192.241.212.223	Port Scan
222.122.51.37	Port Scan	192.241.227.208	Port Scan
80.82.65.90	Port Scan	192.241.222.168	Port Scan
103.133.111.128	Port Scan	192.241.224.64	Port Scan
93.189.43.3	Malware	59.19.147.198	Port Scan
195.3.146.118	Port Scan	176.31.146.23	Port Scan

18.205.93.2	Port Scan	192.241.219.144	Port Scan
18.205.93.0	Port Scan	185.53.88.198	Port Scan
18.205.93.1	Port Scan	192.241.225.107	Port Scan
106.11.250.224	Port Scan	209.126.3.185	Port Scan
106.11.248.90	Port Scan	64.39.99.213	Port Scan
46.243.253.15	Port Scan	45.33.40.145	Port Scan
176.31.6.16	Port Scan	45.33.40.145	Port Scan
108.174.197.76	Port Scan	185.216.140.6	Port Scan
192.236.161.6	Port Scan	192.241.203.89	Port Scan
88.99.242.92	Port Scan	190.210.65.172	Port Scan
185.71.65.238	Port Scan	80.87.199.224	Malware
140.82.52.87	Port Scan	157.52.193.82	Port Scan
45.76.122.92	Port Scan	192.241.228.10	Port Scan
51.38.191.178	Port Scan	192.241.229.86	Port Scan
51.15.56.161	Port Scan	192.241.227.70	Port Scan
158.69.133.18	Port Scan	192.241.222.110	Port Scan
89.35.39.78	Port Scan	46.38.148.22	Port Scan
107.174.47.156	Port Scan	89.248.169.12	Port Scan
83.220.169.247	Port Scan	185.107.80.62	Port Scan
51.38.203.146	Port Scan	185.232.64.32	DDoS
144.217.45.45	Port Scan	185.234.217.241	DDoS
107.174.47.181	Port Scan	185.234.217.8	DDoS
176.31.6.16	Port Scan	185.234.218.225	DDoS
163.172.206.67	Port Scan	185.234.219.140	DDoS
144.217.45.45	Port Scan	197.4.4.12	Malware
185.53.88.21	Port Scan	101.86.170.36	Malware
80.82.77.227	Port Scan	50.23.197.94	Malware
171.67.71.100	Port Scan	85.143.218.203	Malware
185.27.181.99	Port Scan	85.143.219.230	Malware
163.172.29.13	Port Scan	192.241.203.96	Port Scan
183.207.113.104	Port Scan	192.241.210.211	Port Scan
183.207.113.105	Port Scan	192.227.158.108	Port Scan
192.241.233.72	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.



Actualidad

Procedimiento para adjuntar un archivo EML y cabecera

El correo electrónico es uno de los principales medios utilizados por los ciberdelincuentes para cometer estafas, como el phishing. Para comprobar si un mail es malicioso y analizar su contenido, es necesario tener el detalle completo del correo, el que se conserva en su archivo EML y en la cabecera. Si quieres reportar un phishing con la información completa, adjuntar estos elementos resulta esencial.

Para ver esta campaña, se puede utilizar el siguiente enlace:

<https://www.csirt.gob.cl/recomendaciones/procedimiento-para-adjuntar-un-archivo-eml-y-cabecera/>



Ciberconsejos para evitar malware

El malware es un programa o código malicioso diseñado intencionalmente para causar daño a cualquier clase de dispositivos, por ejemplo, computadoras, teléfonos móviles, dispositivos IoT y a toda una infraestructura de red. Existen distintos tipos de malware, y cada uno ellos tiene una característica y una forma de propagarse diferente.

Las consecuencias podrían ser múltiples; anuncios molestos, robo de datos personales o sensibles, pérdida del control del equipo, envío de correos sin consentimiento, encriptar archivos y otras amenazas dependiendo el tipo de infección.

Si quieres conocer los tipos de malware más comunes y cómo prevenir ingresa al siguiente enlace:
<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-malware/>



Ministerio del Interior y Seguridad Pública

CIBERCONSEJOS PARA EVITAR MALWARE

ALGUNOS TIPOS DE MALWARE:

- VIRUS**
Cuando se ejecuta puede modificar o eliminar datos sin que el usuario se dé cuenta. El virus se copia a sí mismo y se propaga a otros dispositivos en red.
- GUSANO**
Su objetivo principal es infectar un equipo y luego propagarse por la red, infectando la mayor cantidad de máquinas. En algunos casos son portadores de otros malware más peligrosos.

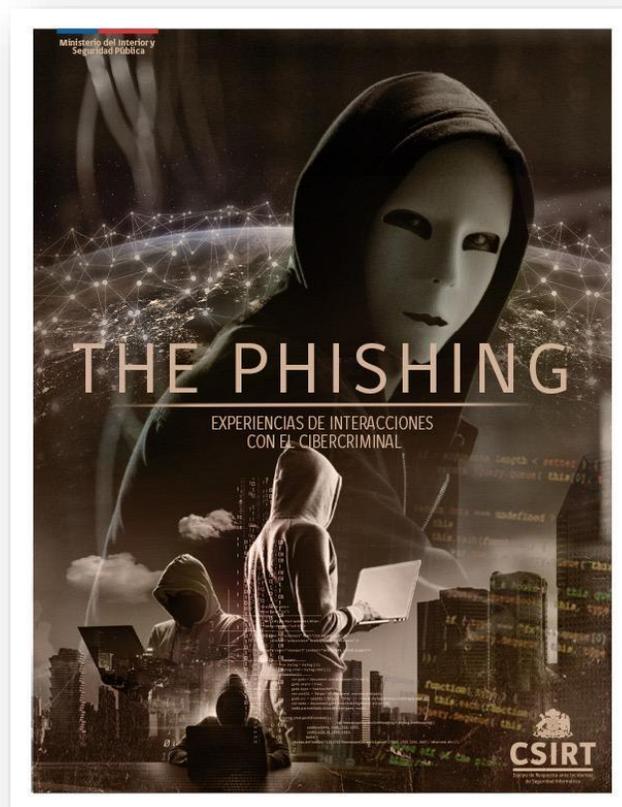
Investigación

Phishing. Experiencias de interacciones con el cibercriminal

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la novena edición de su publicación sobre amenazas cibernéticas el que analiza una serie de interacciones de phishing. Este artículo fue elaborado por Natalia Pérez Muñoz, analista de nivel 2 de CSIRT.

El phishing consiste en el robo de información sensible en línea a través de la suplantación de identidad, en la que los atacantes se hacen pasar por personas o entidades legítimas. Un particular grupo de ellos se realiza a través del uso de técnicas de ingeniería social, solo basado en la interacción con el atacante.

Este trabajo es fruto de una serie de interacciones con cibercriminales a través de intentos de ataques de phishing. Las interacciones entabladas con los atacantes tenían como objetivo encontrar elementos que nos permitieran comprender más sobre el criminal y la víctima. Nuestra investigación se compone de un estudio preliminar y el análisis de 8 encuentros con los atacantes.



Ver en: <https://www.csirt.gob.cl/reportes/an2-2020-09/>

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.

- Cristián Brinck
Linkedin:
www.linkedin.com/in/cristianbrinck/
- Cristóbal Catalán
Linkedin:
- Matia Cornejo
Linkedin:
<https://www.linkedin.com/in/matia-cornejo/>



Resumen anual

El pasado 19 de Junio se cumplió un año desde la primera publicación de este Boletín de Seguridad Cibernética. Su objetivo original, era reunir en un documento la información semanal sobre alertas y vulnerabilidades publicadas en el sitio web y redes sociales de CSIRT.

Queremos acompañar esta edición del Boletín Semanal con una serie de estadísticas que sintetizan la información contenida en un año de publicaciones.

Junto a ello, queremos destacar públicamente a quienes participan permanentemente suministrando el contenido de este documento, específicamente a los analistas de Nivel 2 de CSIRT, Miguel Kurte, Marcelo Latapia, Paula Moraga, Natalia Pérez, Carlos Ramos y Carlos Silva.

De la misma manera, este resumen finaliza con el agradecimiento a todos quienes han aportado a través de nuestro sitio web con información para crear alertas de seguridad cibernética. El agradecimiento es más extenso que los 65 nombres que más abajo se mencionan. También es para quienes en sus roles como responsables de la ciberseguridad de sus organizaciones, ayudan a crear conciencia sobre la importancia de cuidarnos frente a los riesgos y amenazas que existen en el ciberespacio.

Esta publicación nació en 2019 bajo la supervisión del Director del CSIRT, Carlos Landeros Cartes, y del entonces Jefe Operativo de la unidad, Sr. Cristián Berríos Fuentes. La publicación ha continuado e incorporado nuevos elementos desde Enero de 2020, especialmente inclinados a promover la concientización, todo ellos durante la Jefatura del Departamento CSIRT de Katherina Canales Madrid.

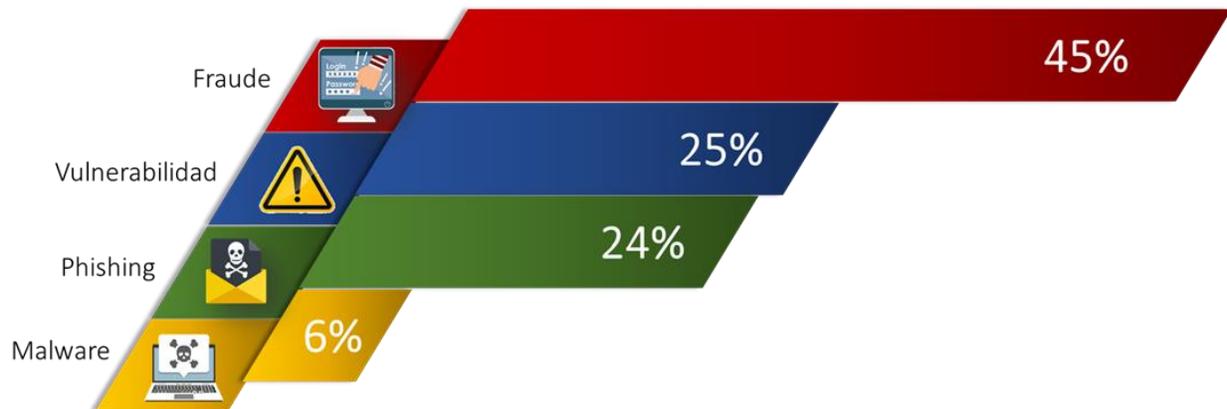
Este Boletín es elaborado semanalmente por el Área de Comunicaciones de CSIRT, específicamente por Carolina Covarrubias y Patricio Quezada, siendo este último su Editor y creador.



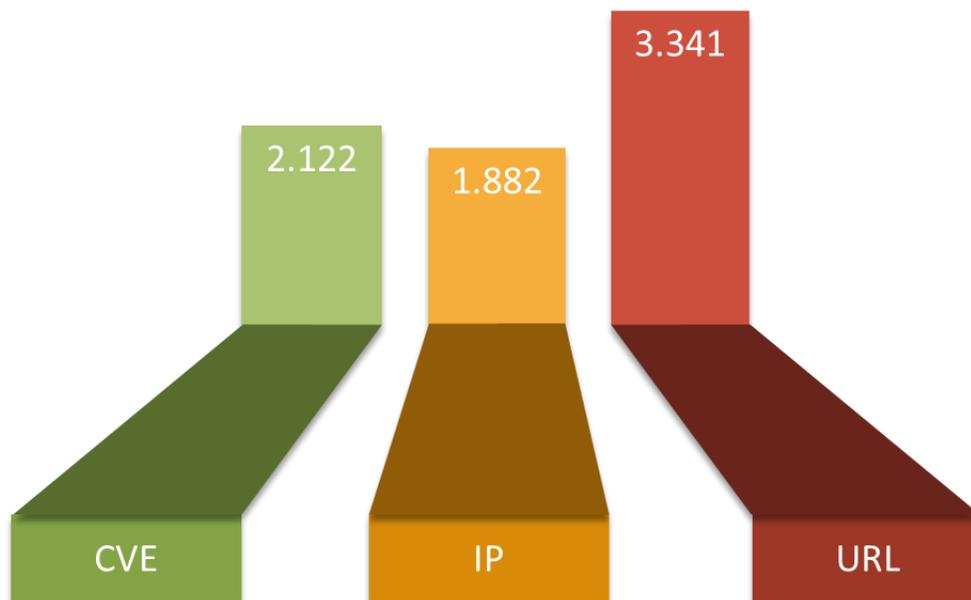
Indicadores generales

En las 51 entregas del Boletín de Ciberseguridad, y distribuidos en 1.011 alertas publicadas, de las cuales 453 fueron fraudes, 249 vulnerabilidades, 245 phishing y 64 malware, fueron compartidos 2.122 parches de seguridad, y advertidas 1.882 IP vinculadas a 3.341 URL de sitios maliciosos.

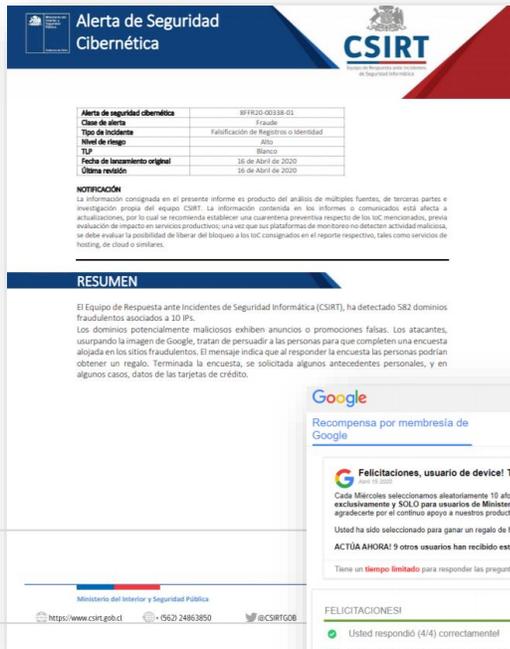
Porcentaje de informes publicados (1.011 en total)



Número de CVE, IP y URL publicadas.



URL informadas por semana



Alerta de Seguridad Cibernética

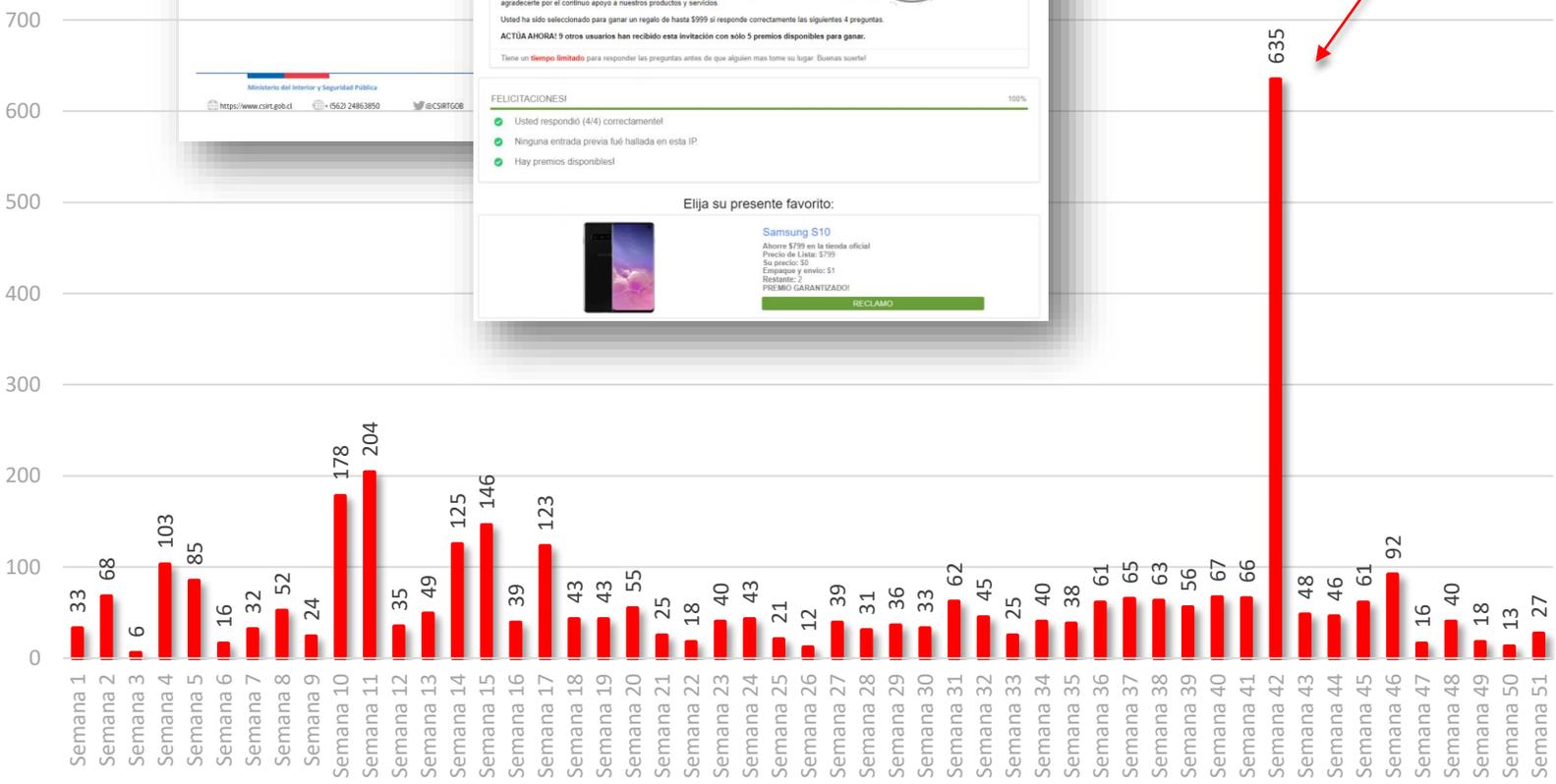
Alerta de seguridad cibernética	8FFR20-00338-01
Clase de alerta	Fraude
Tipo de incidente	Kalificación de registros o identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Abril de 2020
Última revisión	16 de Abril de 2020

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceros partes e investigación propia del equipo CSIRT. La información contenida en los informes y computadores está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IOC mencionados, previa evaluación de impacto en servicios producidos; una vez que los sistemas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar el bloqueo a los IOC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

RESUMEN
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 582 dominios fraudulentos asociados a 3D IPs. Los dominios potencialmente maliciosos exhiben anuncios o promociones falsas. Los atacantes, usurpando la imagen de Google, tratan de persuadir a las personas para que completen una encuesta alojada en los sitios fraudulentos. El mensaje indica que al responder la encuesta las personas podrían obtener un regalo. Terminada la encuesta, se solicitaba algunos antecedentes personales, y en algunos casos, datos de las tarjetas de crédito.

582
Dominios

Fueron informados en la alerta 8FFR20-00338-01 del **16 de abril de 2020**. Los sitios exhibían anuncios y promociones falsas. Los atacantes usurparon la imagen de Google, con el objetivo de que las personas completaran una encuesta. Al finalizar, se solicitaban a la víctima datos personales y, en algunos casos, las tarjetas de crédito.



IP informadas por semana

EMOTET

Este malware estaba asociado a una serie de campañas detectadas e informadas el **23 de septiembre de 2019** en la alerta CMV-00032-001. En total, 222 IP y 74 URL fueron reportadas.

Alerta de Seguridad Informática

Alerta de seguridad informática	2CMV-00032-001
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IOC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IOC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), informa la activación de múltiples campañas de phishing con carga del malware Emotet, con documento tipo Word adjuntos. El fenómeno ha sido recogido por diversos medios informativos de seguridad a nivel mundial. CSIRT ha podido identificar campañas dirigidas especialmente a Chile dentro de este contexto. Este informe se estará ampliando en la medida que se puedan reunir mayor antecedentes. Las fuentes utilizadas en este informe son abiertas. CSIRT quiere llamar la atención a las instituciones públicas y privadas para que tomen las precauciones respectivas y estén alertas a los correos y descargas de archivos.

Ministerio del Interior y Seguridad Pública

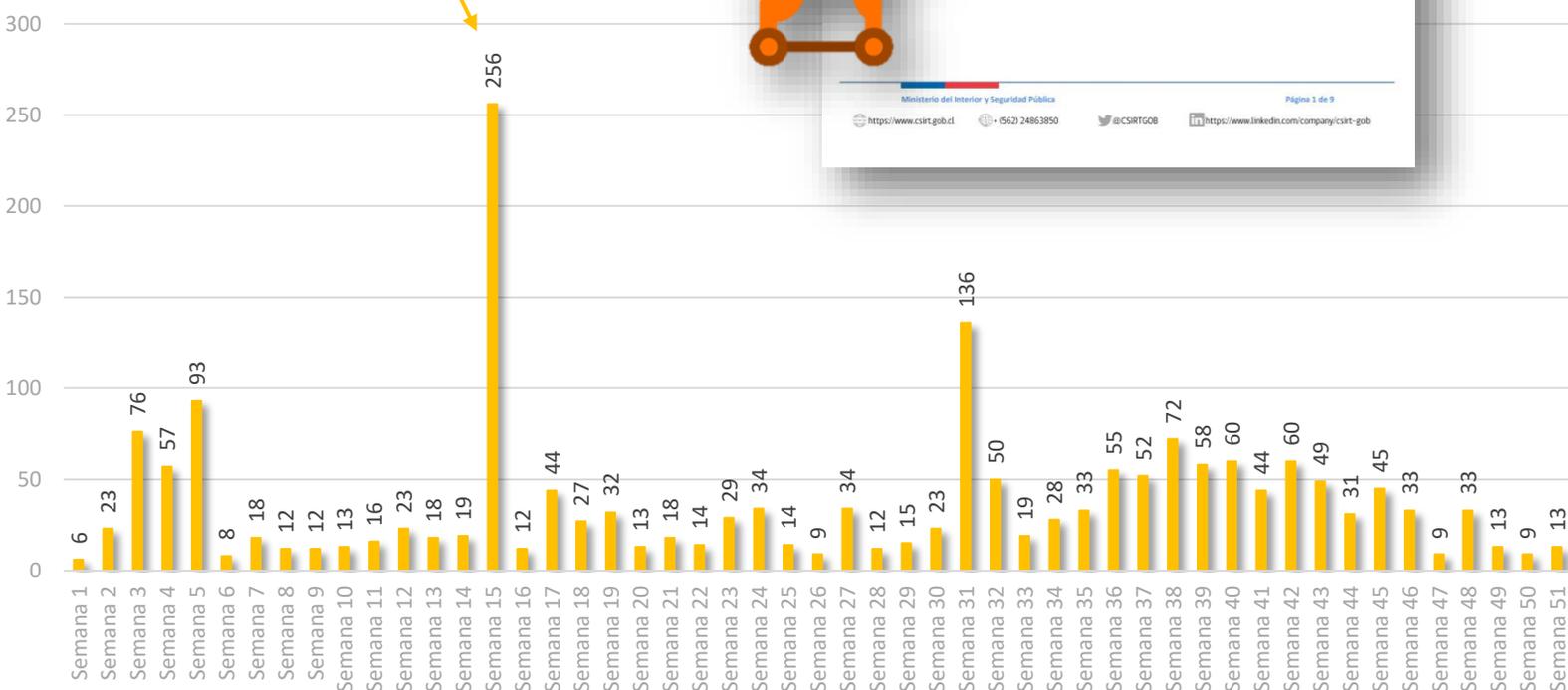
Página 1 de 9

<https://www.csirt.gob.cl>

+ (562) 24863850

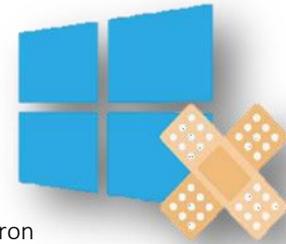
@CSIRTOB

<https://www.linkedin.com/company/csirt-gob>

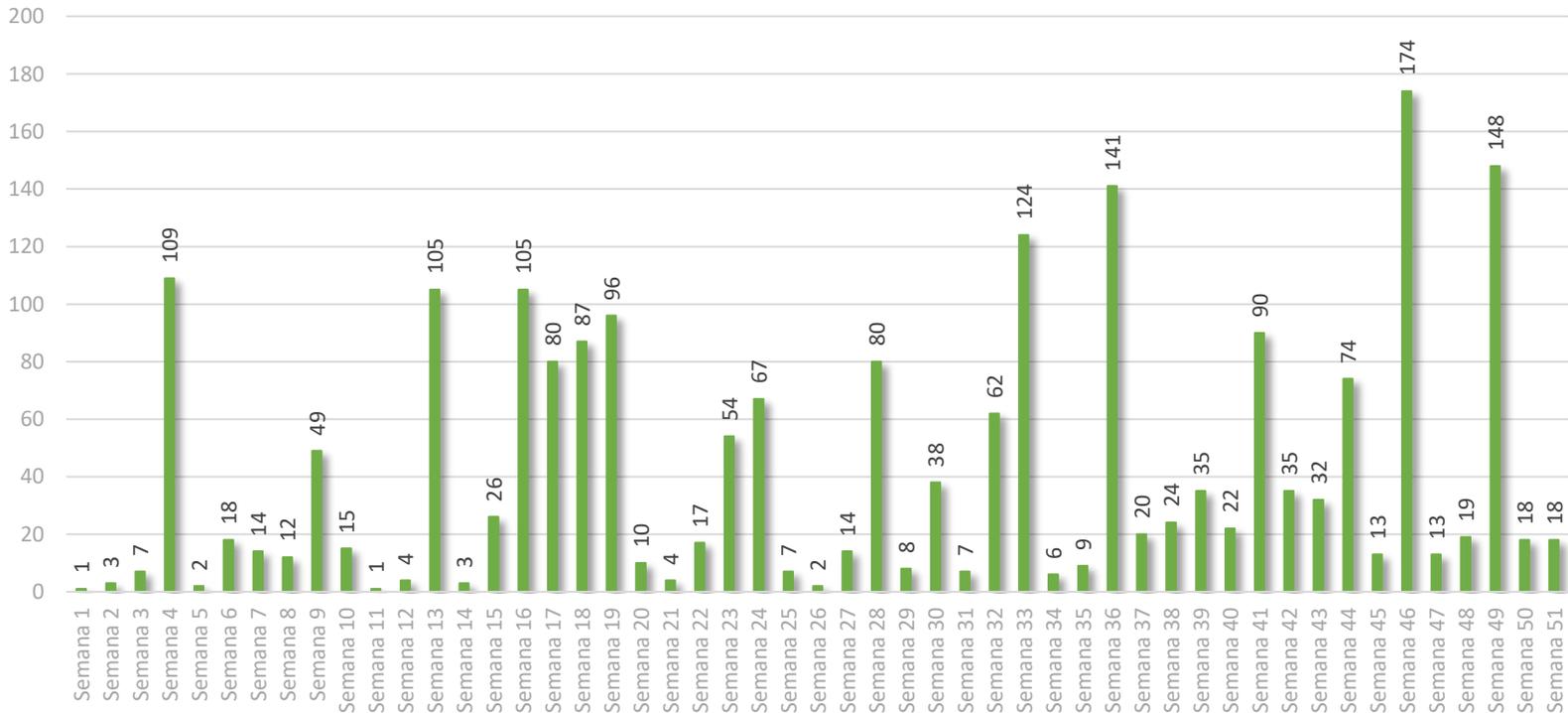


Vulnerabilidades por semana

928



Parches de seguridad fueron obtenidos de **Microsoft** y publicados en los reportes de vulnerabilidad a lo largo de un año. La mayoría de ellos fueron compartidos durante los **Martes de Parche**, el segundo martes de cada mes, y que explica algunas de las cumbres de CVEs en este gráfico.



Investigaciones

9

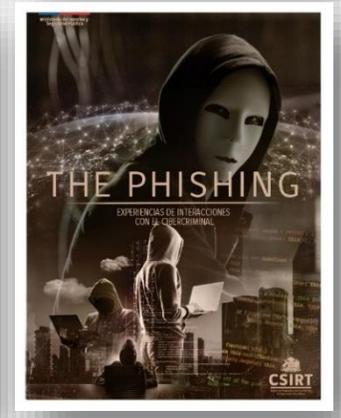
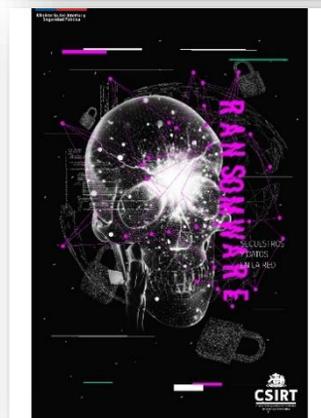
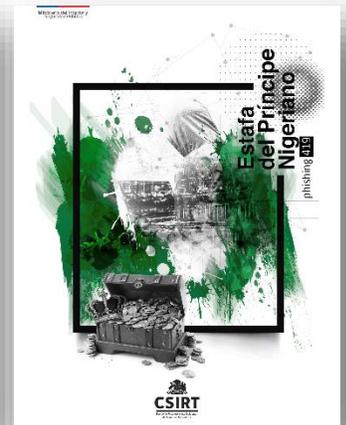
Ediciones de la revista de **Análisis de Amenazas Cibernéticas** han sido publicadas durante 2020, convirtiéndose rápidamente en un aporte a la comunidad de ciberseguridad.

Carlos Silva, Paula Moraga, Natalia Pérez, Juan Moraga, Gabriela Sepúlveda y Hernán Espinoza, todos miembros del CSIRT, figuran entre los autores de estos trabajos.

Las portadas han sido creadas por Jaime Millán.

Para revisar estas publicaciones, pueden ocupar el enlace adjunto:

www.csirt.gob.cl/reportes



Concientización

11

Campañas online ha realizado CSIRT en lo que va del año. Esta es una muestra de las iniciativas de concientización lideras por este Departamento y representa la importancia de crear una cultura cibersegura. Para seguir esta campañas, pueden utilizar el siguiente enlace:

www.csirt.gob.cl/recomendaciones/



CONSEJOS DE CSIRT SEGURIDAD PARA VIDEOCONFERENCIAS

Los medios tecnológicos permiten el despliegue de múltiples herramientas para comunicarse a distancia entre grupos de personas, las que son muy útiles para entornos laborales e institucionales, en particular en momentos que la presencia física se ve dificultada por las condiciones de emergencia sanitaria.

En este contexto, es necesario, considerar un conjunto de criterios que van más allá que la facilidad de instalación y número de usuarios que soporta la plataforma elegida, más aún, si los participantes de dichas reuniones representan a instituciones críticas o sensibles en la organización o coordinación del País o de la actual crisis sanitaria.

Dado que no existe un medio tecnológico libre de estos amenazas y riesgos, el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile CSIRT entregan algunas recomendaciones para que la información que se transmite, al realizar una teleconferencia, pueda desarrollarse de la manera más segura posible.



Ciberconsejos de seguridad Operación Renta 2020

Las phishing más comunes en la Operación Renta

- Revisa el remiteante si recibes un correo electrónico relacionado a la devolución de impuestos o Coronavirus.
- Nunca ingreses tus contraseñas si no confías de un sitio.
- Revisa el contenido, que no sea alarmante o tenga faltas de ortografía.

Para estar preparados, te presentamos los phishing y sitios fraudulentos sobre la Operación Renta de los últimos años.



CIBERATAQUES DIRIGIDOS

¿Cómo prevenir?

- REVISAR el correo del remitente. Los atacantes usan una pequeña variante del correo para parecer legítimo o también hackean cuentas.
- CONFIRMAR la información que recibes, llamando a la persona o al CEO de la empresa.
- NUNCA RESPONDAS este tipo de correos y duda si te solicitan pagos en criptomonedas.
- NO DESCARGUES archivos o abras enlaces de dudosa procedencia, pueden contener malware.
- LIMITA la información que compartas en redes sociales, especialmente para los CEOs.



CIBERCONSEJOS PARA EVITAR DELITOS CIBERNÉTICOS

- NUNCA ENTREGUES las coordenadas de tus tarjetas de transferencias.
- CUIDADO con las ofertas que recibes. Si son muy buenas, duda.
- NUNCA ENTREGUES tus datos financieros.

FONDO DENUNCIA DE CIBERDELITOS 24HRS.
(+562) 2486 3850



CIBERCONSEJOS PARA EVITAR MALWARE

ALGUNOS TIPOS DE MALWARE:

- TROYANO:** Es uno de los malware más peligrosos, ya que se hace pasar por un programa legítimo. Una vez en el sistema, se activa y es posible robar información financiera o instalar otro tipo de malware.
- RANSOMWARE:** Este malware tiene la capacidad de cifrar archivos en sistemas informáticos para pedir rescate de la información sustrahida.
- SPYWARE:** Malware que espía los sistemas informáticos y a sus usuarios, y se las comunica al autor. Se puede utilizar para el registro de claves y actividades similares.



CUIDATE DE LA SEXTORSION



CIBERCONSEJOS PARA UNA NAVEGACION SEGURA

- Actualiza tu navegador. Los ciberatacantes aprovechan las vulnerabilidades de los navegadores, por eso se recomienda instalar las últimas versiones para proteger tu equipo.
- Bloquea los anuncios. Algunos anuncios malintencionados en un navegador pueden contener enlaces o contenido malintencionado.



RECOMENDACIONES PARA PROTEGER CONTRASENAS EN RR.SS.

Las redes sociales nos ofrecen la oportunidad de compartir lo que hacemos diariamente, por lo tanto se han transformado en una extensión de nuestra identidad. Por lo mismo, es necesario tomar precauciones para evitar que un tercero tome el control de tus cuentas en internet.

Las cibercriminales están aprovechando la necesidad de información por la emergencia del covid-19 para multiplicar sus ataques. Hoy más que nunca, debemos ser cuidadosos, necesitamos comunicaciones auténticas y verdaderas en RRSS, para no confundir a la ciudadanía. Especial atención deben tener hoy las autoridades de gobierno y las personas de interés público en la privacidad de sus cuentas. CSIRT comparte algunos consejos.



CIBERCONSEJOS DE SEGURIDAD COMPRAS ONLINE

Evita robos y fraudes en tus compras por internet

¿CÓMO CUIDARSE?

- Ten precaución con las ofertas. Un precio demasiado bajo en comparación con el comercio establecido es sospechoso.
- Revisa la reputación u opiniones de la tienda o vendedor en la web. Es recomendable saber qué han comentado otros usuarios sobre un determinado servicio o producto, ya que te puede orientar sobre la veracidad del sitio.



DESINFORMACION

Las redes sociales permiten que los usuarios sean presionados y manipulados por personas ajenas, lo que ha facilitado la difusión de contenido engañoso. Sigue los siguientes consejos para evitar que te engañen estos simples consejos.

- NO difundas noticias sin verificar.
- NO compartas información que no provenga de medios o fuentes oficiales.
- NO compartas mensajes que puedan generar alarma en la población.



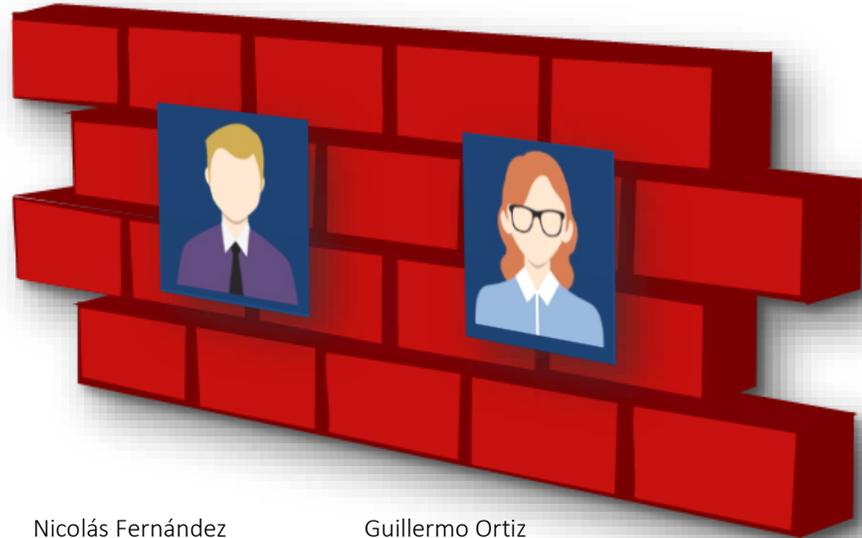
Día Nacional contra el CIBERACOSO

Hay ciberacosos que no se ven. El cyberbullying daña a las personas, ¡no lo aceptes! ¡No seas!

- Defiende y Empatiza.
- Si eres víctima o testigo, DENUNCIA.
- Guía a tus hijos cómo convivir saludablemente en las redes sociales.

Descarga el material en: www.csirt.gob.cl el Abusos Familiar y comenta con tus hijos para que puedan navegar de forma segura por internet.

Muro de la fama 2019-2020



Hernán Aburto
Eduardo Aceto
Luis Miguel Ancapichun
Miguel Ángel Rojas
Diego Arias
Bernardo Avilés
Andrés Basoalto
Rodrigo Benavides
Nicolle Bravo
Felipe Bravo
Mauricio Cabrales
Patricio Campos
Andrés Cargill
Cristián Caris
Dionny Contreras
Matia Cornejo
Rodrigo Cortés
Pablo Cruces Araya
Jaime de los Hoyos
Gabriel Díaz
Abraham Ermann
Alejandro Farías

Nicolás Fernández
Germán Fernández
Eduardo Flores
Tomás Gaete
Gustavo Galleguillos
Manuel González
Víctor Herrera
Cristóbal Herrera
Aaron Jaramillo
Rodrigo Jiménez
Patricio Jofré
Roger Laya
Juan López
Rodrigo Machado Villegas
Milton Matamala
Maurizio Mattoli
Hugo Miranda Vera
Camilo Mix Vásquez
Joaquín Morales
Pablo Olivares
Óscar Orellana
Alejandro Ortega

Guillermo Ortiz
Rodrigo Ostaloza
Felipe Ovalle
Cristián Ovalle Núñez
Jair Palma Vincenty
Ricardo Parra
Claudio Pontigo
Pablo Ramírez
Romel Rivas
Pier Rivera
Eduardo Riveros
Sebastián Romero
Angelo Saavedra Lienan
Jacob Salazar
Kevin Sánchez
Martín Tello Mena
Juan Daniel Tolosa
Francisco Torrijos Jaime
José Vásquez
Benjamin Vega

65

Personas han sido destacadas en esta oportunidad por su contribución desinteresada a la seguridad cibernética de nuestro país. Los destacados semanalmente lo hacen a través de nuestro formulario web. Sin embargo, más personas de las acá mencionadas han aportado, algunas de ellas de forma anónima, y otras en otras vías, como redes sociales. A todos ellos, nuestro reconocimiento y profundo agradecimiento.