09-07-2020 | Año 2 | N°53

Boletín de Seguridad Cibernética

Semana del 02 al 08 de julio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

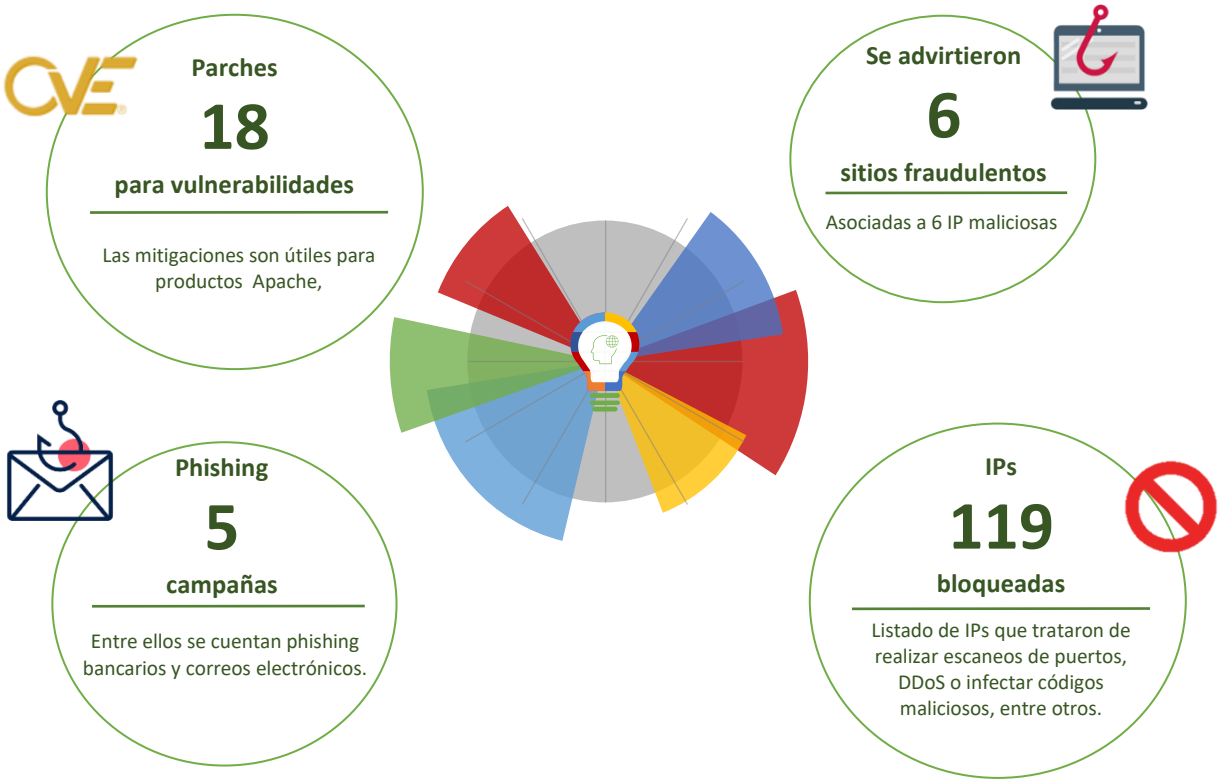
División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras



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

Contenido

Sitios fraudulentos

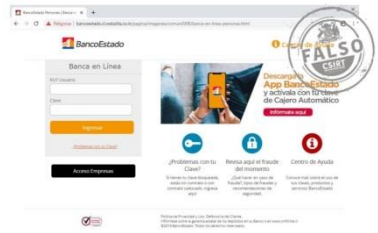
Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00473-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Julio de 2020
Última revisión	02 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://www-bancoestado.cl.scoaladesoferi-azratim[.]ro/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
89.47.53.158	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00473-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00473-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00474-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Julio de 2020
Última revisión	02 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://www-bancoestado.cl.saybolt[.]pl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
91.232.4.250	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00474-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00474-01.pdf	

Imagen del sitio

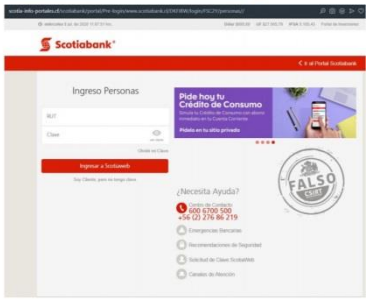


CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00475-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Julio de 2020
Última revisión	06 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://bancoestado.cl.webzilla.co[.]in/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
50.28.57.170	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00475-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00475-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00476-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Julio de 2020
Última revisión	06 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://houseoftaho.com/mants/imagenes/comun2008/banca-en-linea-personas.html	
IP	
107.180.29.18	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00476-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00476-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00477-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Julio de 2020
Última revisión	08 de Julio de 2020
Indicadores de compromiso	
URL	
scotia-info-portales[.]cf	
IP	
91[.]234[.]99[.]114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00477-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00477-01.pdf	

Imagen del sitio

CSIRT advierte sobre portal bancario para fraudes	
Alerta de seguridad cibernética	8FFR20-00478-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Julio de 2020
Última revisión	08 de Julio de 2020
Indicadores de compromiso	
URL	
chile[.]chilesecuritymobile[.]com	
IP	
195[.]189[.]96[.]36	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00478-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00478-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte campaña de phishing por medidas sanitarias	
Alerta de seguridad cibernética	8FPH20-00260-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2020
Última revisión	01 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://ander[.]vn/a[.]php	
hxxps://scotiabnakchile[.]tk/scotiabank/portal/Pre-login/	
IP	
[103.248.146.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00260-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00260-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por cancelación de servicio de streaming	
Alerta de seguridad cibernética	8FPH20-00261-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Julio de 2020
Última revisión	06 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://iplanmyself[.]com/ads/assets/HE/FOVAAA/862112d0626a1372383b328ae7924c7f/	
IP	
[51.15.20.168]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00261-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00261-01.pdf	

Imagen del sitio

CSIRT advierte phishing por crédito bancario	
Alerta de seguridad cibernética	8FPH20-00262-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Julio de 2020
Última revisión	06 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://scotiachile[.]cf/scotiabank/portal/Pre-login/www[.]scotiabankvcl/99HF3N/login/DDSFP/personas//	
IP	
91.234.99.114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00262-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00262-01.pdf	

Imagen del sitio

CSIRT advierte phishing de validación de cuentas en servicio de correo y red social	
Alerta de seguridad cibernética	8FPH20-00263-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Julio de 2020
Última revisión	07 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://been1[.]webnode[.]com/contact/	
IP	
[195.235.225.13]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00263-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00263-01-1.pdf	

Imagen del mensaje

CSIRT informa phishing de cuenta suspendida de un sitio de pago en línea	
Alerta de seguridad cibernética	8FPH20-00264-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Julio de 2020
Última revisión	07 de Julio de 2020
Indicadores de compromiso	
URL	
hxxps://dearcustmireservice[.]berdary[.]com/file/files	
IP	
[173.232.146.83]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00264-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00264-01.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones para ApacheTomcat y ApacheTrafficServer	
Alerta de seguridad cibernética	9VSA20-00259-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Julio de 2020
Última revisión	03 de Julio de 2020
CVE	
CVE-2020-11996 - CVE-2020-9494	
Fabricante	
Apache	
Productos afectados	
Apache Tomcat entre las versiones 10.0.0-M1 y 10.0.0-M5. Apache Tomcat entre las versiones 9.0.0.M1 y 9.0.35. Apache Tomcat entre las versiones 8.5.0 y 8.5.55. pache Traffic Server entre las versiones 6.0.0 y 6.2.3. Apache Traffic Server entre las versiones 7.0.0 y 7.1.10. Apache Traffic Server entre las versiones 8.0.0 y 8.0.7.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00259-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00259-01.pdf	

CSIRT avierte vulnerabilidad y comparte mitigación obtenida de PuTTY	
Alerta de seguridad cibernética	9VSA20-00260-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Julio de 2020
Última revisión	03 de Julio de 2020
CVE	
CVE-2020-14002	
Fabricante	
PuTTY	
Productos afectados	
PuTTY versiones 0.68, 0.69, 0.70, 0.71, 0.72 y 0.73.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00260-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00260-01.pdf	

CSIRT comparte mitigación para vulnerabilidad crítica en interfaz TMUI obtenida de F5	
Alerta de seguridad cibernética	9VSA20-00261-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Julio de 2020
Última revisión	04 de Julio de 2020
CVE	
CVE-2020-5902	
Fabricante	
TMUI	
Producto afectado	
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00261-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00261-01.pdf	

CSIRT comparte mitigaciones para Squid obtenidas de GitHub	
Alerta de seguridad cibernética	9VSA20-00262-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Julio de 2020
Última revisión	08 de Julio de 2020
CVE	
CVE-2020-14059 - CVE-2020-14058 - CVE-2020-15049	
Fabricante	
GitHub	
Productos afectados	
Squid versiones 3.1-3.5.28, 4.0-4.11, 5.0.1-5.0.2. Squid versiones 2.0-2.STABLE9, 3.0-3.5.28, 4.0-4.11, 5.0.1-5.0.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00262-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00262-01.pdf	

CSIRT advierte de vulnerabilidades y comparte mitigaciones para Citrix	
Alerta de seguridad cibernética	9VSA20-00263-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Julio de 2020
Última revisión	08 de Julio de 2020
CVE	
CVE-2019-18177 - CVE-2020-8187 - CVE-2020-8190 CVE-2020-8191 - CVE-2020-8193 - CVE-2020-8194 CVE-2020-8195 - CVE-2020-8196 - CVE-2020-8197 CVE-2020-8198 - CVE-2020-8199	
Fabricante	
Citrix	
Producto afectado	
Citrix ADC y Citrix Gateway. Citrix ADC y Citrix Gateway versiones 12.0 y 11.1. Citrix ADC, Citrix Gateway y Citrix SDWAN WAN-OP modelos 4000-WO, 4100-WO, 5000-WO y 5100-WO.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00263-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00263-01.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
62.210.177.52	Port Scan	192.241.214.26	Port Scan
185.39.11.105	Port Scan	208.115.215.190	Port Scan
192.241.225.109	Port Scan	192.241.229.102	Port Scan
209.141.41.177	Port Scan	192.241.222.207	Port Scan
192.95.37.71	Port Scan	37.49.230.250	Port Scan
185.56.81.52	Port Scan	37.49.230.159	Port Scan
163.172.9.38	Port Scan	37.49.224.3	Port Scan
192.241.216.95	Port Scan	37.49.224.147	Port Scan
192.241.224.135	Port Scan	37.49.230.47	Port Scan
192.241.216.229	Port Scan	37.49.224.59	Port Scan
80.82.70.140	Port Scan	37.49.224.38	Port Scan
67.21.79.138	Port Scan	37.49.230.133	Port Scan
192.241.228.142	Port Scan	37.49.230.158	Port Scan
192.241.212.203	Port Scan	37.49.230.252	Port Scan
192.241.230.250	Port Scan	37.49.224.19	Port Scan
78.18.200.74	Port Scan	192.241.224.137	Port Scan
192.241.227.150	Port Scan	151.236.63.229	Port Scan
192.241.214.64	Port Scan	62.210.189.183	Port Scan
192.241.222.97	Port Scan	77.247.110.28	Port Scan
192.241.225.206	Port Scan	93.174.93.94	Port Scan
192.241.219.171	Port Scan	192.241.228.148	Port Scan
192.241.194.119	Port Scan	192.241.222.157	Port Scan
192.241.229.237	Port Scan	134.119.221.5	Port Scan
2.57.122.98	Port Scan	192.158.239.129	Port Scan
93.174.93.197	Port Scan	14.102.254.230	Port Scan
185.36.81.239	Port Scan	192.241.224.219	Port Scan
37.49.230.159	Port Scan	156.96.47.131	Port Scan
45.148.121.78	Port Scan	192.241.228.141	Port Scan
31.187.78.6	Port Scan	198.199.92.224	Port Scan
192.241.219.54	Port Scan	192.241.219.42	Port Scan

89.248.168.244	Port Scan	192.241.228.22	Port Scan
45.143.220.31	Port Scan	93.174.89.53	Hacking
192.241.224.206	Port Scan	192.241.230.238	Port Scan
158.69.155.80	Port Scan	192.241.224.123	Port Scan
192.241.196.70	Port Scan	79.174.23.130	Port Scan
192.241.192.197	Port Scan	192.241.219.66	Port Scan
192.241.224.136	Port Scan	45.143.220.65	Port Scan
192.241.222.235	Port Scan	211.72.17.17	Port Scan
192.241.225.123	Port Scan	92.63.197.95	Port Scan
192.241.212.58	Port Scan	89.248.167.141	Port Scan
185.53.88.65	Port Scan	192.241.224.66	Port Scan
198.199.104.250	Port Scan	63.143.32.122	Port Scan
92.39.29.101	Port Scan	192.241.228.40	Port Scan
45.14.224.120	Port Scan	192.241.222.109	Port Scan
195.154.40.99	Port Scan	192.241.229.143	Port Scan
192.241.227.101	Port Scan	45.148.121.84	Port Scan
192.241.229.107	Port Scan	103.1.72.89	Port Scan
209.141.55.247	Port Scan	83.66.113.180	Port Scan
45.143.220.74	Port Scan	209.141.62.69	Port Scan
173.212.87.151	Port Scan	5.182.210.206	Port Scan
45.148.121.11	Port Scan	37.49.224.28	Port Scan
68.183.105.162	Port Scan	110.13.149.126	Port Scan
163.172.206.6	Port Scan	157.52.193.73	Port Scan
192.241.224.33	Port Scan	164.132.91.99	Port Scan
178.21.164.90	Port Scan	103.11.135.50	Port Scan
94.102.49.82	Port Scan	192.241.214.186	Port Scan
94.102.49.114	Port Scan	181.199.102.179	Malware
192.241.225.55	Port Scan	192.241.227.31	Port Scan
185.53.88.203	Port Scan	192.241.217.26	Port Scan
192.241.224.82	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.

Concientización

Publicación especial "Cibersucesos"

El CSIRT lanzó una publicación con interesantes temas de investigación, tendencias digitales y concientización, con el fin de acercar los temas del ciberespacio a la ciudadanía.

CIBERSUCESOS es la primera publicación del Gobierno en Chile en materia de concientización en ciberseguridad, en la cual se exponen temas muy contingentes, ya que la crisis sanitaria ha puesto en evidencia la necesidad de contar con tecnologías que permitan darle continuidad, dentro de lo posible, a ciertas actividades del día a día, sin dejar de lado la ciberseguridad, tanto para las personas como organizaciones e instituciones.

Ver en:
https://www.csirt.gob.cl/

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.

- Víctor Cárdenas
- Alexei Morales
  Linkedin:
  https://www.linkedin.com/in/alexeimorales/
- Renzo Cataldo
  Linkedin:
  https://www.linkedin.com/in/renzo-cataldo-orsini-3b981532/

CSIRT Gobierno de Chile Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.07.09 18:21:54 -04'00'