CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 6 de Diciembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 28 de Noviembre y el miércoles 04 de Diciembre.

Falsificación de Registro o Identidad

8FFR-00129-001 CSIRT ADVIERTE LA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00129-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2019
Última revisión	27 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00129-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00129-001.pdf

8FFR-00130-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00119-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2019
Última revisión	22 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco de Chile, el que podría servir para robar credenciales de usuarios de esa entidad.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00130-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00130-001.pdf

8FFR-00120-001 CSIRT ADVIERTE SOBRE ACTIVACIÓN DE 4 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00130-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Noviembre de 2019
Última revisión	28 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales bancarios fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco de Chile, lo que podría servir para el robo de credenciales de usuarios de esa entidad.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00120-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00120-001.pdf

8FFR-00131-001 CSIRT ADVIERTE DE SUPLANTACIÓN DE SITIO DE OPERADOR DE TARJETAS

Alerta de seguridad informática	8FFR-00121-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2019
Última revisión	23 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de CMR Falabella, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad comercial aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00131-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00131-001.pdf

8FFR-00132-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00132-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2019
Última revisión	29 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Santander, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00132-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00132-001.pdf

8FFR-00133-001 CSIRT ADVIERTE LA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00133-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Noviembre de 2019
Última revisión	29 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Itaú, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00133-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00133-001.pdf

8FFR-00134-001 CSIRT ADVIERTE DE ACTIVACIÓN DE NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00134-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Noviembre de 2019
Última revisión	30 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00134-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00134-001.pdf

8FFR-00135-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00135-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de Diciembre de 2019
Última revisión	1 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00135-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00135-001.pdf

8FFR-00136-001 CSIRT ADVIERTE DE 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00136-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de Diciembre de 2019
Última revisión	2 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 3 portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/media/2019/12/8FFR-00136-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00136-001/

8FFR-00137-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00137-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de Diciembre de 2019
Última revisión	3 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00137-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00137-001.pdf

8FFR-00138-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR-00138-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de Diciembre de 2019
Última revisión	4 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Scotiabank, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00138-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00138-001.pdf

8FFR-00139-001 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00139-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de Diciembre de 2019
Última revisión	4 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a dos IP que suplantan el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00139-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00139-001-.pdf

Vulnerabilidades

9VSA-00092-001 CSIRT COMPARTE ACTUALIZACIONES PARA MOZILLA NSS

Alerta de seguridad informática	9VSA-00092-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	30 de noviembre de 2019
Última revisión	30 de noviembre de 2019

Vulnerabilidad

CVE-2019-11745

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Mozilla, referente a una vulnerabilidad que afecta a servicios de seguridad de red, la cual, si es explotada, puede resultar en ejecución de código remoto. Adjunto en este informe se publican los enlaces para descargar las respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00092-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00092-001.pdf

9VSA-00093-001 CSIRT COMPARTE ACTUALIZACIONES PARA F5

Alerta de seguridad informática	9VSA-00093-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2019
Última revisión	22 de noviembre de 2019

Vulnerabilidad

CVE-2019-6665
CVE-2019-6672
CVE-2019-6674
CVE-2019-6667
CVE-2019-6666
CVE-2019-6669
CVE-2019-6673
CVE-2019-6668
CVE-2019-6671

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por F5 referente a diversas vulnerabilidades presentes en sus productos.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00093-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00093-001.pdf

9VSA-00094-001 CSIRT COMPARTE ACTUALIZACIONES PARA SQUID

Alerta de seguridad informática	9VSA-00094-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de diciembre de 2019
Última revisión	2 de diciembre de 2019

Vulnerabilidad

CVE-2019-12526
CVE-2019-12523
CVE-2019-18676
CVE-2019-18677
CVE-2019-18678
CVE-2019-18679

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Squid, referente a vulnerabilidades que afectan a sus servidores Proxy, las cuales, si son explotadas, pueden resultar en ataques de denegación de servicios, exposición de información y hasta ejecución de código remoto. Esto junto a su respectiva actualización para mitigar los riesgos.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00094-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00094-001.pdf

9VSA-00095-001 CSIRT COMPARTE ACTUALIZACIONES PARA DJANGO

Alerta de seguridad informática	9VSA-00095-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de diciembre de 2019
Última revisión	3 de diciembre de 2019

Vulnerabilidad
CVE-2019-19118
Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Django, referente a una vulnerabilidad que afecta a su framework web, la cual, de ser explotada, puede resultar en escalación de privilegios. El informe incluye las actualizaciones para mitigar el riesgo.
Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00095-001-2/
https://www.csirt.gob.cl/media/2019/12/9VSA-00095-001.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados 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
114.67.237.246	Port scan
106.54.137.185	Port scan
106.51.44.69	Port scan
103.47.192.146	Port scan
103.126.101.47	Port scan
61.220.175.233	Port scan
61.219.41.144	Port scan
61.178.128.9	Port scan
49.234.178.89	Port scan
49.232.45.168	Port scan
47.254.29.6	Port scan
45.40.203.33	Port scan

45.40.192.150	Port scan
43.226.147.87	Port scan
40.125.200.20	Port scan
218.7.110.129	Port scan
183.111.108.12	Port scan
167.86.106.92	Port scan
154.8.200.196	Port scan
153.3.250.139	Port scan
148.70.233.219	Port scan
140.238.159.183	Port scan
14.33.247.248	Port scan
139.199.22.202	Port scan
139.155.99.228	Port scan
139.155.2.188	Port scan
124.239.176.49	Port scan
123.206.30.169	Port scan
122.136.212.216	Port scan
122.114.31.174	Port scan
122.114.189.12	Port scan
118.24.221.245	Port scan
116.228.105.86	Port scan
114.34.108.193	Port scan
111.231.227.135	Port scan
111.230.182.13	Port scan
106.13.82.113	Port scan
111.185.236.5	Port scan
110.10.40.199	Port scan
106.53.92.202	Port scan
106.12.69.20	Port scan
103.86.49.187	Port scan
103.78.243.153	Port scan
103.226.126.69	Port scan
101.51.106.223	Port scan
85.51.149.32	Port scan
62.234.97.157	Port scan
51.38.33.178	Port scan
51.15.112.47	Port scan
49.234.177.135	Port scan
45.113.160.13	Port scan
43.226.54.34	Port scan
41.60.245.37	Port scan

27.124.22.185	Port scan
23.224.45.82	Port scan
202.28.62.209	Port scan
2.59.153.91	Port scan
193.112.203.71	Port scan
181.206.77.3	Port scan
185.216.119.90	Port scan
159.192.96.109	Malware
140.143.204.199	Malware
132.145.27.239	Malware
130.61.77.253	Malware
129.28.90.29	Malware
129.211.134.62	Malware
123.58.133.21	Malware
122.97.215.50	Malware
122.114.235.78	Malware
121.201.61.248	Malware
118.25.112.198	Malware
111.231.194.181	Malware
106.13.33.80	Malware
106.13.100.181	Malware
103.56.113.208	Malware
103.37.234.169	Malware
103.238.163.140	Malware
103.204.179.171	Malware
103.204.177.146	Malware
103.100.211.106	Malware
94.191.113.146	Malware
61.19.34.18	Malware
59.127.238.44	Malware
49.235.155.55	Malware
45.40.196.167	Malware
193.112.185.115	Malware
187.188.83.115	Malware
185.216.119.65	Malware
183.131.120.30	Malware
172.81.254.221	Malware
154.218.1.233	Malware
129.28.203.203	Malware
124.40.246.1	Malware
123.206.191.254	Malware

122.114.127.128	Malware
121.133.252.253	Malware
119.29.94.177	Malware
119.29.81.238	Malware
119.29.157.216	Malware
118.24.182.64	Malware
117.18.12.68	Malware
116.196.118.116	Malware
115.124.110.200	Malware
111.231.225.7	Malware
106.75.193.16	Malware
106.13.83.26	Malware
106.13.58.36	Malware
106.13.184.202	Malware
103.76.85.190	Malware
103.71.51.12	Malware
103.60.221.149	Malware
103.218.3.21	Malware
103.200.28.122	Malware
103.105.58.219	Malware
103.100.210.23	Malware
94.191.126.118	Malware
94.191.121.117	Malware
93.84.86.69	Malware
61.135.192.72	Malware
58.87.115.217	Malware
51.89.100.98	Malware
49.254.0.172	Malware
49.235.141.111	Malware
49.234.230.5	Malware
49.234.178.155	Malware
45.195.25.158	Malware
27.124.40.217	Malware
220.179.138.9	Malware
218.25.89.93	Malware
202.52.14.74	Malware
202.166.163.115	Malware
202.108.199.62	Malware
192.144.164.111	Malware
190.27.251.237	Malware
182.243.91.146	Malware

150.109.67.14	Malware
150.109.108.102	Malware
139.199.9.231	Malware
139.199.179.239	Malware
139.199.17.13	Malware
134.175.45.222	Malware
129.28.159.3	Malware
129.28.148.105	Malware
129.28.121.194	Malware
129.226.63.10	Malware
124.172.153.21	Malware
124.106.83.63	Malware
122.51.91.181	Malware
121.243.17.150	Malware
119.29.96.35	Malware
118.24.23.164	Malware
115.84.105.161	Malware
112.30.132.178	Malware
112.29.171.57	Malware
111.231.65.134	Malware
110.72.251.22	Malware
106.53.108.72	Malware
106.52.192.63	Malware
106.13.71.209	Malware
106.13.137.54	Malware
106.12.40.185	Malware
106.12.187.27	Malware
106.12.156.233	Malware
106.12.141.136	Malware
103.86.66.186	Malware
103.55.30.58	Malware
103.139.1.203	Malware
103.100.208.242	Malware
94.191.19.188	Malware
91.83.165.179	Malware
62.234.157.189	Malware
62.234.156.87	Malware
62.234.111.129	Malware
59.46.170.118	Malware
49.235.178.217	Malware
47.251.49.39	Malware

43.252.231.141	Malware
39.109.17.36	Malware
39.109.116.53	Malware
27.124.47.221	Malware
49.248.92.246	Malware
89.144.47.4	Malware
202.129.206.186	Malware
202.100.78.114	Malware
192.144.230.143	Malware
185.245.43.88	Malware
183.134.74.13	Malware
182.254.162.69	Hacking
180.76.146.109	Hacking
139.199.34.191	Hacking
139.199.219.241	Hacking
139.199.176.149	Hacking
129.28.206.38	Port scan
129.28.150.88	Port scan
129.28.137.27	Port scan
123.30.236.77	Port scan
122.189.200.90	Port scan
119.28.222.106	Port scan
118.24.49.139	Port scan
118.24.169.221	Port scan
111.231.201.221	Port scan
111.230.67.238	Port scan
106.54.229.217	Port scan
103.94.181.68	Port scan
103.90.203.250	Port scan
103.76.87.30	Port scan
103.60.222.113	Port scan
103.55.26.213	Port scan
103.123.160.199	Port scan
94.191.127.232	Port scan
87.139.108.253	Port scan
60.190.202.39	Port scan
58.244.255.35	Port scan
49.235.182.95	Port scan
49.233.73.178	Port scan
45.93.17.135	Port scan
45.40.204.206	Port scan

45.137.17.228	Port scan
42.51.13.12	Port scan
39.109.104.200	Port scan
219.251.34.3	Port scan
219.152.171.128	Port scan
218.89.107.200	Hacking
218.255.173.218	Hacking
206.222.2.2	Port scan
173.45.68.90	Port scan
51.89.125.71	Port scan
188.92.75.248	Port scan
185.246.128.26	Port scan
193.105.134.95	Port scan
204.42.253.132	Port scan
188.92.77.235	Port scan
184.105.109.246	Port scan
176.123.5.120	Port scan
94.102.51.87	Port scan
51.159.59.47	Port scan
146.88.240.128	Port scan
93.174.93.4	Port scan
184.105.139.85	Port scan
184.105.139.89	Port scan
184.105.139.101	Port scan

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.06 16:34:43 -03'00'