13BCS20-00035-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 03 de Enero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 26 de Diciembre de 2019 y el miércoles 01 de Enero de 2020.

Falsificación de Registro o Identidad

8FFR-00166-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR-00166-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2019
Última revisión	27 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 BCI, 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://csirt.gob.cl/alertas/8ffr-00166-001/

https://csirt.gob.cl/media/2019/12/8FFR-00166-001.pdf

8FFR-00167-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00167-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2019
Última revisión	27 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 suplantan 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://csirt.gob.cl/alertas/8ffr-00167-001/
https://csirt.gob.cl/media/2019/12/8FFR-00167-001.pdf

8FFR-00168-001 ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00168-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de diciembre de 2019
Última revisión	28 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 BCI, 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://csirt.gob.cl/alertas/8ffr-00168-001/
https://csirt.gob.cl/media/2019/12/8FFR-00168-001.pdf

8FFR-00169-001 CSIRT ADVIERTE ACTIVACIÓN DE 3 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00169-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2019
Última revisión	31 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 tres IP que suplantan el sitio web oficial de Banco Estado, los que podrían servir para robar credenciales de usuarios de esa entidad.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios del servicio y a la entidad aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr-00169-001/
https://csirt.gob.cl/media/2019/12/8FFR-00169-001.pdf

8FFR-00170-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00170-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2019
Última revisión	31 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado un portal fraudulento asociado a una IP que ha sido utilizada para suplantar el sitio web oficial del Banco Falabella, con el propósito de robar credenciales de usuarios de esa entidad u otras acciones maliciosas.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://csirt.gob.cl/alertas/8ffr-00170-001/
https://csirt.gob.cl/media/2019/12/8FFR-00170-001.pdf

8FPH-00078-001 CSIRT ADVIERTE DE PHISHING POR BLOQUEO TEMPORAL DE CUENTA

Alerta de seguridad informática	8FPH-00078-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2019
Última revisión	30 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Estado. El correo indica que los servidores de procesos fueron actualizados y que se encuentran operativos, sin embargo, la cuenta del usuario no se encuentra registrada, por lo que se se procedió al bloqueo temporal de la misma. Los estafadores disponibilizan un enlace para restaurar la cuenta, incitando a sus víctimas a ingresar al vínculo, de lo contrario, el usuario necesitara ir a la sucursal para el desbloqueo. El enlace lo direcciona a un sitio semejante al del Banco.

Enlace:

https://csirt.gob.cl/alertas/8fph-00078-001/
https://csirt.gob.cl/media/2019/12/8FPH-00078-001.pdf

8FPH-00079-001 CSIRT ADVIERTE PHISHING POR MANTENIMIENTO DE SERVICIOS BANCARIOS

Alerta de seguridad informática	8FPH-00079-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2019
Última revisión	30 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Estado. El correo indica que se realizó un mantenimiento de los servicios Caja Vecina, ServiEstado y la aplicación móvil, encontrando un error en la cuenta. Debido a esto se procedió con el bloqueo de la cuenta. Los estafadores disponibilizan un enlace para restaurar la cuenta, incitando a sus víctimas a ingresar al vínculo e indicando que es la única forma de desbloquear la cuenta. El enlace redirecciona al usuario a un sitio semejante al del Banco.

Enlace:

https://csirt.gob.cl/alertas/8fph-00079-001/
https://csirt.gob.cl/media/2019/12/8FPH-00079-001.pdf

Vulnerabilidades

9VSA-00109-001 CSIRT COMPARTE ACTUALIZACIONES PARA APACHE

Alerta de seguridad informática	9VSA-00109-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2019
Última revisión	30 de diciembre de 2019

Vulnerabilidad

CVE-2019-17558

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de la fuente oficial de Apache, referente a una vulnerabilidad que afecta a Apache Solr, la cual, de ser explotada, permitiría a un atacante remoto ejecutar código en el contexto de la aplicación. El informe contiene la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa-00109-001/
https://csirt.gob.cl/media/2019/12/9VSA-00109-001.pdf

9VSA-00110-001 CSIRT COMPARTE ACTUALIZACIONES DE BIG-IP(ASM) DE F5

Alerta de seguridad informática	9VSA-00110-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de diciembre de 2019
Última revisión	31 de diciembre de 2019

Vulnerabilidad

CVE-2019-6682

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por F5 referente a una vulnerabilidad que afecta a su producto BIG-IP(ASM). El informe incluye un enlace para descargar la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa-00110-001/
https://csirt.gob.cl/media/2019/12/9VSA-00110-001.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante las pasadas dos semanas 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
37.49.231.182	Port Scan
47.75.98.123	Port Scan
84.205.241.3	Port Scan
113.190.242.52	Port Scan
45.143.220.128	Port Scan
144.91.82.35	Port Scan
115.74.224.8	Port Scan
115.74.246.179	Port Scan
163.172.99.57	Port Scan
142.93.61.111	Port Scan
45.56.78.64	Port Scan
51.91.247.125	Port Scan
92.118.161.13	Port Scan
192.99.152.160	Port Scan
217.182.204.72	Port Scan
80.211.173.73	Port Scan
37.49.230.102	Port Scan
212.237.25.99	Port Scan
80.211.224.49	Port Scan
80.211.57.210	Port Scan
80.211.72.186	Port Scan
80.211.29.59	Port Scan
216.66.22.2	Port Scan
192.68.128.206	Port Scan
209.131.128.219	Port Scan
209.131.128.217	Port Scan
185.12.179.187	Port Scan
209.131.128.215	Port Scan
209.131.128.211	Port Scan
209.131.128.204	Port Scan
185.12.179.187	Port Scan
209.131.128.215	Port Scan
209.131.128.211	Port Scan

209.131.128.204	Port Scan
185.200.118.86	Port Scan
163.47.142.250	Port Scan
104.244.75.222	Port Scan
93.56.28.7	Port Scan
194.182.88.78	Port Scan
93.174.93.216	Port Scan
37.49.230.67	Port Scan
68.183.128.171	Port Scan
103.36.18.164	Port Scan
163.172.6.254	Port Scan
144.91.83.1	Port Scan
45.148.10.12	Port Scan
195.231.2.225	Port Scan
218.212.229.168	Port Scan
58.182.177.119	Port Scan
188.25.56.16	Port Scan
125.214.51.158	Port Scan
84.94.197.28	Port Scan
212.224.77.58	Port Scan
82.118.242.42	Port Scan
217.61.61.246	Port Scan
185.200.118.37	Port Scan
195.154.26.99	Port Scan
80.211.172.24	Port Scan
151.217.112.34	Port Scan
151.217.28.28	Port Scan
103.40.163.221	Port Scan
37.49.231.181	Port Scan
204.152.201.239	Port Scan
61.222.248.187	Port Scan
14.227.190.180	Port Scan
45.143.220.137	Port Scan
185.200.118.82	Port Scan
77.247.109.55	Port Scan
196.52.84.34	Port Scan
145.239.204.11	Port Scan
202.79.168.37	Port Scan
77.247.110.183	Port Scan
103.103.161.66	Port Scan
120.29.118.70	Port Scan

151.217.117.35	Port Scan
107.6.91.26	Port Scan
191.33.228.130	Port Scan
68.183.123.115	Port Scan
151.217.176.13	Port Scan
151.217.117.49	Port Scan
185.200.118.67	Port Scan
195.154.194.179	Port Scan
195.201.77.108	Port Scan
92.195.163.75	Port Scan
204.48.22.80	Port Scan
151.217.176.85	Port Scan
168.196.201.147	Port Scan
151.217.111.81	Port Scan
188.85.27.107	Port Scan
212.71.255.214	Port Scan
151.217.177.192	Port Scan
60.225.63.80	Port Scan
183.82.32.189	Port Scan
188.26.185.12	Port Scan
58.182.186.177	Port Scan
116.87.206.133	Port Scan
177.84.153.161	Port Scan
103.212.140.93	Port Scan
185.43.209.207	Port Scan
109.92.137.166	Port Scan
144.91.82.223	Port Scan
58.82.233.158	Port Scan
151.217.119.127	Port Scan
68.183.128.156	Port Scan
209.150.146.221	Port Scan
209.150.146.216	Port Scan
216.245.219.212	Port Scan
151.217.143.72	Port Scan
151.217.111.121	Port Scan
151.217.23.89	Port Scan
151.217.117.64	Port Scan
151.217.176.75	Port Scan
151.217.177.210	Port Scan
151.217.139.77	Port Scan
59.152.220.84	Port Scan

116.105.228.10	Port Scan
54.36.60.191	Port Scan
54.36.60.191	Port Scan
151.217.101.94	Port Scan
185.134.49.94	Port Scan
178.128.144.17	Port Scan
151.217.28.27	Port Scan
151.217.111.201	Port Scan
151.217.176.170	Port Scan
37.49.231.162	Port Scan
211.216.208.63	Port Scan
151.217.178.149	Port Scan
163.172.9.30	Port Scan
163.152.43.238	Port Scan
202.39.9.153	Port Scan
45.195.25.86	Port Scan
151.217.178.102	Port Scan
151.217.178.44	Port Scan
194.32.117.3	Port Scan
62.210.178.126	Port Scan
151.217.141.111	Port Scan
37.49.229.170	Port Scan
83.110.81.134	Port Scan
185.153.197.162	Port Scan
79.124.8.102	Port Scan
159.203.30.120	Port Scan
194.32.117.3	Port Scan
151.217.119.160	Port Scan
151.217.178.40	Port Scan
118.91.161.246	Port Scan
212.83.144.8	Port Scan
151.217.119.170	Port Scan
79.222.111.30	Port Scan
92.42.44.118	Port Scan
113.182.125.3	Port Scan
115.74.203.230	Port Scan
128.14.181.70	Port Scan
176.235.216.98	Port Scan
212.83.147.11	Port Scan
212.237.46.158	Port Scan
51.15.147.80	Port Scan

62.210.180.226	Port Scan
151.217.179.2	Port Scan
45.43.236.214	Hacking
45.227.253.36	Hacking
151.217.119.176	Port Scan
151.217.141.127	Port Scan
129.208.23.243	Port Scan
45.143.220.143	Port Scan
104.238.111.142	Port Scan
124.105.239.169	Port Scan
139.99.28.174	Port Scan
149.129.68.54	Port Scan
151.217.176.235	Port Scan
151.217.176.247	Port Scan
151.217.178.193	Port Scan
151.217.178.89	Port Scan
172.83.156.107	Port Scan
185.172.110.214	Port Scan
192.236.193.107	Port Scan
193.70.14.116	Port Scan
45.67.14.148	Port Scan
80.211.185.190	Port Scan
80.211.152.232	Port Scan
89.46.72.100	Port Scan
101.127.56.144	Port Scan
116.87.40.136	Port Scan
14.239.60.37	Port Scan
191.5.0.188	Port Scan
222.164.42.47	Port Scan
58.182.164.23	Port Scan
162.241.60.177	Phishing
195.231.4.50	Port Scan
176.113.70.51	Port Scan
68.183.128.202	Port Scan
117.54.15.253	Port Scan
68.183.86.76	Port Scan
167.99.203.202	Port Scan
157.245.126.61	Port Scan
216.218.206.66	Port Scan
94.23.11.131	Port Scan
195.231.0.238	Port Scan

139.162.195.60	Port Scan
37.49.231.183	Port Scan
59.96.199.89	Port Scan
46.109.135.218	Port Scan
14.231.164.205	Port Scan
37.49.230.105	Port Scan
27.254.190.106	Port Scan
1.53.197.133	Port Scan
51.159.59.241	Port Scan
176.58.112.254	Port Scan
69.164.213.180	Port Scan
62.210.6.56	Port Scan
92.222.204.120	Port Scan
103.71.255.70	Port Scan
82.102.173.83	Port Scan
51.38.140.27	Port Scan
163.152.52.81	Port Scan
103.234.138.250	Port Scan
188.166.240.171	Port Scan

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.

- Martín Tello Mena
- Hernán Aburto - https://www.linkedin.com/in/hernanaburto/
- Maurizio Mattoli - https://www.linkedin.com/in/mauriziomattoli/

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: 2020.01.03 12:27:11 -03'00'