

13BCS-00033-001

## CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática  
Publicado el Viernes 20 de Diciembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 12 y el miércoles 18 de Diciembre.

### Falsificación de Registro o Identidad

#### 8FFR-00148-001 CSIRT ADVIERTE ACTIVACIÓN DE TRES PORTALES FRAUDULENTOS

Alerta de seguridad informática	8FFR-00148-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Diciembre de 2019
Última revisión	12 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 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-00148-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00148-001.docx.pdf>

### 8FFR-00149-001 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00149-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Diciembre de 2019
Última revisión	13 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 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-00149-001/>  
<https://www.csirt.gob.cl/media/2019/12/8FFR-00149-001.pdf>

### 8FFR-00150-001 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00150-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2019
Última revisión	14 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 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-00150-001/>  
<https://www.csirt.gob.cl/media/2019/12/8FFR-00150-001.pdf>

### 8FFR-00151-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00151-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Diciembre de 2019
Última revisión	14 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 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 del servicio y a la entidad aludida.

#### Enlace:

<https://www.csirt.gob.cl/alertas/8ffr-00151-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00151-001.pdf>

### 8FFR-00152-001 CSIRT ADVIERTE ACTIVACIÓN DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00152-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de diciembre de 2019
Última revisión	16 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 una 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-00152-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00152-001.pdf>

### 8FFR-00153-001 CSIRT ADVIERTE ACTIVACIÓN DE CUATROS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00153-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de diciembre de 2019
Última revisión	17 de diciembre de 2019

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a una IP, los 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 y a la entidad aludida.

### Enlace:

<https://www.csirt.gob.cl/alertas/8ffr-00153-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00153-001.pdf>

### 8FFR-00154-001 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00154-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de diciembre de 2019
Última revisión	17 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 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-00154-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00154-001.docx.pdf>

### 8FFR-00155-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00155-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de diciembre de 2019
Última revisión	18 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 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 y a la entidad aludida.

### Enlace:

<https://www.csirt.gob.cl/alertas/8ffr-00155-001/>

<https://www.csirt.gob.cl/media/2019/12/8FFR-00155-001.pdf>

## Alertas de Phishing

### 8FPH-00077-001 CSIRT ADVIERTE SOBRE CAMPAÑA DE PHISHING CON DIVERSOS MENSAJES

Alerta de seguridad informática	8FPH-00077-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Diciembre de 2019
Última revisión	17 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 que intenta persuadir a los usuarios del Banco Scotiabank, para seleccionar un hipervínculo que los direcciona a un sitio semejante al del Banco. Para ello, los atacantes utilizan diversos mensajes en el cuerpo del correo para convencer a la víctima de seleccionar el enlace, cómo por ejemplo:

Que su cuenta se le descontó \$300.000 pesos por un incumplimiento de un pago

Que la cuenta fue suspendida por no realizar un pago de impuestos

Que se le descontó \$450.000 pesos por un error en los sistemas

Que su tarjeta de crédito por realizar una operación sospechosa se procedió a su bloqueo

### Enlace

<https://www.csirt.gob.cl/alertas/8fph-00077-001/>

<https://www.csirt.gob.cl/media/2019/12/8FPH-00077-001.pdf>

## Alertas de Malware

## 2CMV-00041-001 CSIRT ADVIERTE DE CAMPAÑA DE MALWARE-EMOTET

Alerta de seguridad informática	2CMV-00041-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Diciembre de 2019
Última revisión	11 de Diciembre de 2019

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Malware-Emotet. La campaña se activa a partir de archivos .doc que se encuentran almacenados en sitios nacionales vulnerados, los que al ser ejecutados por el usuario, gatillan un script que establece contacto con sitios internacionales desde los que se descargan archivos que desencadenan la infección.

### Enlace

<https://www.csirt.gob.cl/alertas/2cmv-00041-001/>

<https://www.csirt.gob.cl/media/2019/12/2CMV-00041-001.pdf>

## Vulnerabilidades

### 9VSA-00099-001 CSIRT COMPARTE 36 PARCHES ENTREGADOS POR MICROSOFT PARA SUS PRODUCTOS

Alerta de seguridad informática	9VSA-00099-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2019
Última revisión	12 de diciembre de 2019

### Vulnerabilidad

CVE-2019-1332  
 CVE-2019-1349  
 CVE-2019-1350  
 CVE-2019-1351  
 CVE-2019-1352  
 CVE-2019-1354  
 CVE-2019-1387  
 CVE-2019-1400  
 CVE-2019-1453  
 CVE-2019-1458  
 CVE-2019-1461  
 CVE-2019-1462  
 CVE-2019-1463

CVE-2019-1464  
 CVE-2019-1465  
 CVE-2019-1466  
 CVE-2019-1467  
 CVE-2019-1468  
 CVE-2019-1469  
 CVE-2019-1470  
 CVE-2019-1471  
 CVE-2019-1472  
 CVE-2019-1474  
 CVE-2019-1476  
 CVE-2019-1477  
 CVE-2019-1478  
 CVE-2019-1480  
 CVE-2019-1481  
 CVE-2019-1483  
 CVE-2019-1484  
 CVE-2019-1485  
 CVE-2019-1486  
 CVE -2019-1487  
 CVE-2019-1488  
 CVE-2019-1489  
 CVE-2019-1490

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a Diciembre del 2019, en el que pone a disposición del público un total de 36 parches para mitigar vulnerabilidades en sus softwares.

**Enlace**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa-00099-001/>  
<https://www.csirt.gob.cl/media/2019/12/9VSA-00100-001.docx.pdf>

**9VSA-00100-001 CSIRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS ADOBE**

Alerta de seguridad informática	9VSA-00100-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de diciembre de 2019
Última revisión	12 de diciembre de 2019

**Vulnerabilidad**

CVE-2019-8256

CVE-2019-8255  
 CVE-2019-8253  
 CVE-2019-8254  
 CVE-2019-16449  
 CVE-2019-16456  
 CVE-2019-16457  
 CVE-2019-16458  
 CVE-2019-16461  
 CVE-2019-16465  
 CVE-2019-16450  
 CVE-2019-16454  
 CVE-2019-16445  
 CVE-2019-16448  
 CVE-2019-16452  
 CVE-2019-16459  
 CVE-2019-16464  
 CVE-2019-16451  
 CVE-2019-16462  
 CVE-2019-16446  
 CVE-2019-16455  
 CVE-2019-16460  
 CVE-2019-16463  
 CVE-2019-16444  
 CVE-2019-16453

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por Adobe, referente a vulnerabilidades que afectan a sus productos.

**Enlace**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa-00100-001/>  
<https://www.csirt.gob.cl/media/2019/12/9VSA-00100-001.docx.pdf>

**9VSA-00101-001 CSIRT COMPARTE ACTUALIZACIONES PARA REDHAT Y SU PRODUCTO OPENSIFT**

Alerta de seguridad informática	9VSA-00101-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de diciembre de 2019
Última revisión	17 de diciembre de 2019

**Vulnerabilidad**

CVE-2019-10432  
 CVE-2019-10431  
 CVE-2019-11255  
 CVE-2017-18367  
 CVE-2019-11250



## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por Redhat, referente a vulnerabilidades que afectan a su producto OpenShift Container Platform.

## Enlace

<https://www.csirt.gob.cl/vulnerabilidades/9vsa-00101-001/>

<https://www.csirt.gob.cl/media/2019/12/9VSA-00101-001.docx.pdf>

## 9VSA-00102-001 CSIRT COMPARTE ACTUALIZACIÓN PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA-00102-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de diciembre de 2019
Última revisión	18 de diciembre de 2019

## Vulnerabilidad

CVE-2019-13767

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por Google, referente a una vulnerabilidad que afecta al explorador Google Chrome. En este informe también se encuentra la correspondiente mitigación.

## Enlace

<https://www.csirt.gob.cl/vulnerabilidades/9vsa-00102-001/>

<https://www.csirt.gob.cl/media/2019/12/9VSA-00102-001.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 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
188.138.125.155	Port Scan
104.40.149.33	Port Scan
59.145.117.130	Port Scan
37.49.230.57	Port Scan
144.217.93.8	Port Scan
176.25.4.240	Port Scan
103.248.37.28	Port Scan
154.221.20.38	Port Scan
187.202.217.203	Port Scan

112.196.21.3	Port Scan
94.102.56.151	Port Scan
176.113.70.34	Port Scan
137.220.174.2	Port Scan
151.80.109.223	Port Scan
36.72.167.93	Port Scan
81.201.58.151	Port Scan
77.247.109.47	Port Scan
219.250.188.71	Port Scan
171.100.23.62	Port Scan
50.116.123.7	Port Scan
188.166.119.234	Port Scan
77.247.109.48	Port Scan
183.91.7.38	Port Scan
173.249.13.175	Port Scan
122.166.167.244	Port Scan
178.128.108.19	Port Scan
182.176.221.162	Port Scan
163.172.9.16	Port Scan
134.209.110.34	Port Scan
103.115.44.214	Port Scan
156.220.18.33	Port Scan
178.128.97.75	Port Scan
203.163.249.75	Port Scan
134.209.110.44	Port Scan
159.203.197.17	Port Scan
103.125.19.2	Port Scan
103.140.182.2	Port Scan
116.97.87.88	Port Scan
121.7.25.159	Port Scan
163.152.183.30	Port Scan
37.49.231.103	Port Scan
43.229.226.58	Port Scan
213.174.157.150	Phishing
124.104.50.102	Port Scan
45.27.247.144	Port Scan
93.104.210.68	Port Scan
62.114.122.156	Port Scan
149.56.206.101	Port Scan
201.183.227.129	Port Scan
212.129.34.195	Port Scan

203.254.158.46	Port Scan
105.159.55.219	Port Scan
51.89.52.208	Port Scan
103.15.106.243	Port Scan
163.27.222.96	Port Scan
103.4.165.73	Port Scan
123.28.90.87	Port Scan
201.103.108.155	Port Scan
14.162.198.45	Port Scan
37.49.230.95	Port Scan
144.217.207.15	Port Scan
162.144.57.42	Port Scan
217.61.106.64	Port Scan
37.49.230.70	Port Scan
45.143.221.31	Port Scan
47.52.204.46	Port Scan
62.210.77.158	Port Scan
92.118.37.64	Port Scan
77.247.109.43	Port Scan
89.248.168.62	Port Scan
107.155.55.70	Port Scan
66.220.151.249	Port Scan
142.93.217.47	Phishing
94.193.100.121	Port Scan
42.116.10.220	Port Scan
189.170.43.58	Port Scan
115.160.252.246	Port Scan
185.132.249.208	Port Scan
197.46.94.238	Port Scan
138.99.216.147	Port Scan
77.247.109.74	Port Scan
159.203.197.156	Port Scan
86.50.252.154	Port Scan
14.191.153.95	Port Scan
110.137.100.233	Port Scan
35.180.41.51	Port Scan
179.43.149.174	Port Scan
62.210.116.103	Port Scan
103.100.208.233	Port Scan
222.239.87.76	Port Scan
83.97.20.164	Port Scan

194.55.187.3	Port Scan
194.55.187.131	Port Scan
83.97.20.162	Port Scan
88.130.220.140	Port Scan
47.56.147.15	Port Scan
139.0.31.10	Port Scan
195.154.220.114	Port Scan
184.106.81.166	Port Scan
103.79.143.181	Port Scan
41.230.67.205	Port Scan
101.127.183.208	Port Scan
116.86.191.32	Port Scan
116.86.207.208	Port Scan
58.182.11.198	Port Scan
58.182.134.101	Port Scan
58.182.137.130	Port Scan
45.143.220.76	Port Scan
58.96.208.227	Port Scan
188.26.91.33	Port Scan
177.72.47.145	Port Scan
188.25.37.192	Port Scan
138.75.112.144	Port Scan
1.22.207.10	Port Scan
51.77.56.9	Port Scan
185.237.18.21	Port Scan
64.62.134.220	Port Scan
172.104.94.121	Port Scan
176.105.254.234	Port Scan
140.109.28.108	Port Scan
45.136.108.111	Port Scan

URL	Motivo
<a href="https://boiler-horizontal.[.]com/wp-admin/SdTbTO/">https://boiler-horizontal.[.]com/wp-admin/SdTbTO/</a>	Malware
<a href="http://fedomede.[.]com/wp-content/danvv6/">http://fedomede.[.]com/wp-content/danvv6/</a>	Malware
<a href="http://acqua.[.]solarcytec.[.]com/rtsbgs/XiWmtYYur/">http://acqua.[.]solarcytec.[.]com/rtsbgs/XiWmtYYur/</a>	Malware
<a href="https://blog.[.]learncy.[.]net/wp-admin/user/oxZqQp/">https://blog.[.]learncy.[.]net/wp-admin/user/oxZqQp/</a>	Malware
<a href="https://sg771.[.]kwikfunnels.[.]com/phpmyadmin_bck/x9tfn-lv1h4-174129596">https://sg771.[.]kwikfunnels.[.]com/phpmyadmin_bck/x9tfn-lv1h4-174129596</a>	Malware
<a href="http://www.[.]4celia.[.]com/wp-admin/2z8/- CS 10000302753 - 13/12/2019">http://www.[.]4celia.[.]com/wp-admin/2z8/- CS 10000302753 - 13/12/2019</a>	Malware
<a href="http://capsaciphone.[.]com/wp-admin/q07360/">http://capsaciphone.[.]com/wp-admin/q07360/</a>	Malware
<a href="http://www.[.]yadegarebastan.[.]com/wp-content/mhear/">http://www.[.]yadegarebastan.[.]com/wp-content/mhear/</a>	Malware
<a href="http://bikerzonebd.[.]com/wp-admin/89gw/">http://bikerzonebd.[.]com/wp-admin/89gw/</a>	Malware

<a href="http://shptoys.com/_old/bvGej/">http://shptoys.com/_old/bvGej/</a>	Malware
<a href="http://www.vestalicom.com/facturation/qgm0t/">http://www.vestalicom.com/facturation/qgm0t/</a>	Malware
<a href="https://www.activacion-bancoestadocl.info/imagenes/comun2008/banca-en-linea-personas.php?html">https://www.activacion-bancoestadocl.info/imagenes/comun2008/banca-en-linea-personas.php?html</a>	Phishing

## 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.

- Camilo Mix - <https://www.linkedin.com/in/lixah/>

## 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