13BCS-00029-001

# CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 21 de Noviembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 14 y el miércoles 20 de Noviembre.

## Falsificación de Registro o Identidad

### 8FFR-00110-001 CSIRT ADVIERTE DE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00110-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de Noviembre de 2019 |
| Última revisión | 14 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-00110-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00110-001.docx.pdf

## 8FFR-00111-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00111-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de Noviembre de 2019 |
| Última revisión | 14 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-00101-001-2/
https://www.csirt.gob.cl/media/2019/11/8FFR-00111-001.pdf

## 8FFR-00112-001 CSIRT ADVIERTE SOBRE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00112-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 16 de Noviembre de 2019 |
| Última revisión | 16 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 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-00112-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00112-001.pdf

## 8FFR-00113-001 CSIRT ADVIERTE DE 37 PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00113-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 16 de Noviembre de 2019 |
| Última revisión | 16 de Noviembre de 2019 |

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 37 portales fraudulentos asociado a una IP, los que suplantan el sitio web oficial de Banco de Chile, y 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, clientes y a la entidad bancaria aludida.

### Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00113-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00113-001.pdf

## 8FFR-00114-001 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00114-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 17 de Noviembre de 2019 |
| Última revisión | 17 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 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-00114-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00114-001.pdf

## 8FFR-00115-001 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00115-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 18 de Noviembre de 2019 |
| Última revisión | 18 de Noviembre 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 suplantan el sitio web oficial de Banco Scotiabank, lo 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-00115-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00115-001.pdf

## 8FFR-00116-001 CSIRT INFORMA LA ACTIVACIÓN DE PORTAL FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00116-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Noviembre de 2019 |
| Última revisión | 19 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 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-00116-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00116-001.docx.pdf

### 8FFR-00117-001 CSIRT ADVIERTE DE SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad informática | 8FFR-00117-001 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Noviembre de 2019 |
| Última revisión | 20 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 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-00117-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00117-001.pdf

## Vulnerabilidades

### 9VSA-00086-001 CSIRT COMPARTE ACTUALIZACIONES PARA VMWARE

| | |
|---|---|
| Alerta de seguridad informática | 9VSA-00086-001 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Medio |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de noviembre de 2019 |
| Última revisión | 15 de noviembre de 2019 |

**Vulnerabilidad**

CVE-2019-5540
CVE-2019-5541
CVE-2019-5542
CVE-2018-12207
CVE-2019-11135
CVE-2018-12126
CVE-2018-12127
CVE-2018-12130
CVE-2019-11091

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMware, referente a vulnerabilidades en sus diferentes productos, las cuales permiten a una atacante local generar ataques de tipo Denegación de Servicios, ejecución de código y obtención de información sin autenticación. También se comparte sus respectivas formas de mitigarlas

**Enlace**

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00086-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00086-002.docx.pdf

**9VSA-00087-001 CSIRT COMPARTE ACTUALIZACIONES PARA WHATSAPP**

| | |
|---|---|
| Alerta de seguridad informática | 9VSA-00087-001 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de noviembre de 2019 |
| Última revisión | 19 de noviembre de 2019 |

**Vulnerabilidad**

CVE-2019-11931

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Facebook referente a una vulnerabilidad presente en su cliente de mensajería WhatsApp.

**Enlace**

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00087-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00087-001.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 |
|---|---|
| 185.112.147.18 | Port Scan |
| 210.19.254.175 | Port Scan |
| 159.203.197.175 | Port Scan |
| 125.227.23.199 | Hacking |
| 103.123.160.220 | Hacking |
| 23.228.73.181 | Port Scan |
| 23.228.73.182 | Port Scan |
| 23.228.73.184 | Port Scan |

| | |
|---|---|
| 77.247.110.173 | Port Scan |
| 222.112.107.46 | Port Scan |
| 103.248.86.26 | Port Scan |
| 103.73.96.241 | Port Scan |
| 206.72.197.90 | Port Scan |
| 37.49.231.109 | Port Scan |
| 68.66.224.54 | Phishing |
| 185.209.0.17 | Port Scan |
| 185.209.0.16 | Port Scan |
| 185.209.0.33 | Port Scan |
| 94.247.244.120 | Port Scan |
| 77.243.115.154 | Port Scan |
| 144.91.195.208 | Port Scan |
| 185.153.196.240 | Port Scan |
| 185.153.199.131 | Port Scan |
| 185.153.199.134 | Port Scan |
| 185.153.199.130 | Port Scan |
| 185.153.199.132 | Port Scan |
| 185.153.199.133 | Port Scan |
| 185.153.199.2 | Port Scan |
| 144.139.158.155 | Malware |
| 46.29.183.211 | Malware |
| 201.163.74.202 | Malware |
| 217.199.160.224 | Malware |
| 68.183.190.199 | Malware |
| 80.85.87.122 | Malware |
| 86.42.166.147 | Malware |
| 89.188.124.145 | Malware |
| 91.204.163.19 | Malware |
| 88.250.223.190 | Malware |
| 154.120.227.206 | Malware |
| 190.4.50.26 | Malware |
| 201.190.133.235 | Malware |
| 200.58.83.179 | Malware |
| 81.213.215.216 | Malware |
| 76.69.29.42 | Malware |
| 190.146.131.105 | Malware |
| 181.16.17.210 | Malware |
| 220.241.38.226 | Malware |
| 41.75.135.93 | Malware |
| 170.130.31.177 | Malware |
| 51.255.165.160 | Malware |

| | |
|---|---|
| 163.172.40.218 | Malware |
| 111.119.233.65 | Malware |
| 182.176.106.43 | Malware |
| 186.47.82.6 | Malware |
| 177.105.242.229 | Malware |
| 186.10.243.34 | Malware |
| 186.10.243.70 | Malware |
| 190.128.222.14 | Malware |
| 103.205.177.229 | Malware |
| 104.238.80.237 | Malware |
| 157.7.164.178 | Malware |
| 189.218.243.150 | Malware |
| 201.196.15.79 | Malware |
| 152.169.32.143 | Malware |
| 192.163.221.191 | Malware |
| 193.34.144.138 | Malware |
| 198.57.217.170 | Malware |
| 211.229.116.130 | Malware |
| 46.105.131.68 | Malware |
| 91.109.5.28 | Malware |
| 138.197.140.163 | Malware |
| 187.177.155.123 | Malware |
| 172.104.143.39 | Malware |
| 172.93.100.154 | Malware |
| 138.68.212.113 | Malware |
| 163.30.54.10 | Malware |
| 45.143.220.34 | Port Scan |
| 209.141.43.166 | Port Scan |
| 209.141.48.177 | Port Scan |
| 193.32.163.102 | Port Scan |
| 134.209.89.22 | Port Scan |
| 178.128.250.18 | Port Scan |
| 178.62.30.41 | Port Scan |
| 82.102.173.73 | Port Scan |
| 193.169.254.34 | Port Scan |
| 185.234.219.43 | Port Scan |
| 178.128.255.8 | Port Scan |
| 209.99.40.221 | Malware |
| 208.100.26.234 | Malware |
| 194.58.56.142 | Malware |
| 195.22.26.248 | Malware |
| 184.105.192.2 | Malware |

| | |
|---|---|
| 185.12.177.206 | Hacking |
| 185.12.177.100 | Hacking |
| 23.228.73.179 | Port Scan |
| 23.228.73.189 | Port Scan |
| 80.211.129.33 | Phishing |
| 91.209.70.108 | Phishing |
| 62.219.50.252 | Malware |
| 159.203.193.242 | Malware |
| 185.176.27.242 | Malware |
| 211.43.220.254 | Malware |
| 138.197.5.224 | Hacking |
| 185.176.221.164 | Port Scan |
| 104.248.3.54 | Port Scan |
| 45.95.168.102 | Port Scan |
| 110.4.46.102 | Hacking |
| 159.203.193.245 | Port Scan |
| 185.242.4.205 | DDoS |
| 45.143.220.57 | Port Scan |
| 139.59.91.113 | Port Scan |
| 163.172.240.197 | Port Scan |
| 51.68.181.196 | Port Scan |
| 103.110.81.249 | Port Scan |
| 45.248.69.46 | Port Scan |
| 45.143.221.7 | Port Scan |
| 192.157.246.106 | Port Scan |
| 139.162.206.243 | Port Scan |
| 209.17.97.58 | Port Scan |
| 45.79.49.77 | Port Scan |
| 27.75.115.14 | Port Scan |
| 37.49.231.122 | Port Scan |
| 80.85.86.175 | Port Scan |
| 107.6.183.138 | Port Scan |
| 107.6.183.162 | Port Scan |
| 113.181.193.97 | Port Scan |
| 159.203.197.172 | Port Scan |
| 163.30.20.3 | Port Scan |
| 184.154.139.12 | Port Scan |
| 216.244.66.230 | Port Scan |
| 220.134.209.152 | Port Scan |
| 185.53.88.4 | Port Scan |
| 202.79.174.158 | Port Scan |
| 104.148.87.125 | Hacking |

| | |
|---|---|
| 159.203.197.9 | Port Scan |
| 185.176.27.2 | Port Scan |
| 116.202.23.152 | Port Scan |
| 104.248.87.195 | Port Scan |
| 94.102.57.187 | Port Scan |
| 51.91.172.227 | Port Scan |
| 159.203.193.43 | Port Scan |
| 45.136.111.65 | Port Scan |
| 89.248.174.193 | Port Scan |
| 27.110.223.180 | Port Scan |
| 185.200.118.57 | Port Scan |
| 149.129.100.135 | Port Scan |
| 179.184.16.47 | Port Scan |
| 54.38.155.103 | Port Scan |
| 173.249.35.45 | Port Scan |
| 27.74.243.12 | Hacking |
| 46.235.42.105 | Hacking |
| 83.97.20.49 | Port Scan |
| 92.118.37.91 | Port Scan |
| 77.247.109.35 | Port Scan |
| 159.203.197.10 | Port Scan |
| 68.183.217.62 | Hacking |
| 159.203.197.157 | Port Scan |
| 160.153.153.158 | Hacking |
| 198.251.80.199 | Malware |
| 163.47.140.92 | Malware |
| 185.234.37.207 | Port Scan |
| 183.88.63.80 | Port Scan |
| 49.49.66.128 | Port Scan |
| 187.189.73.59 | Port Scan |
| 183.89.113.93 | Port Scan |
| 41.73.9.101 | Port Scan |
| 14.207.42.178 | Port Scan |
| 190.13.83.100 | Port Scan |
| 103.129.222.173 | Port Scan |
| 182.253.235.215 | Port Scan |
| 107.180.109.11 | Hacking |
| 46.161.27.150 | DDOS |
| 74.82.47.2 | DDOS |
| 35.194.185.36 | DDOS |
| 47.244.14.192 | Port Scan |
| 212.47.234.231 | Port Scan |

| | |
|---|---|
| 154.66.217.26 | Port Scan |
| 179.185.114.203 | Port Scan |
| 43.242.242.196 | Port Scan |
| 103.209.131.3 | Port Scan |
| 51.158.120.84 | Port Scan |
| 163.172.147.94 | Port Scan |
| 103.216.95.16 | Port Scan |
| 31.169.65.90 | Port Scan |
| 103.250.166.4 | Port Scan |
| 45.32.129.35 | Port Scan |
| 115.186.178.150 | Port Scan |
| 183.89.60.198 | Port Scan |
| 27.116.51.119 | Port Scan |
| 109.226.52.213 | Port Scan |
| 103.75.209.222 | Port Scan |
| 103.28.121.58 | Port Scan |
| 144.217.74.219 | Port Scan |
| 140.227.230.89 | Port Scan |
| 81.23.32.47 | Port Scan |
| 149.28.139.82 | Port Scan |
| 124.156.119.21 | Port Scan |
| 150.109.55.190 | Port Scan |
| 52.187.121.7 | Port Scan |
| 51.89.229.233 | Port Scan |
| 45.143.221.12 | Port Scan |
| 80.82.77.235 | Port Scan |

| URL | Motivo |
|---|---|
| hxxps[://]scotiabank[.]viewdns.net/index | Phishing |

## 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

# Campaña

El CSIRT quiere promover una campaña para no confundirse con el bombardeo de información falsa que circula en redes sociales. El llamado es, ANTES DE VIRALIZAR, VERIFICAR. La información falsa puede generar confusión, llevarnos a tomar decisiones erradas o generar conflictos.


CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.22 09:09:34 -03'00'