CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 28 de Febrero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 20 de Febrero y el miércoles 26 de Febrero de 2020.

Falsificación de Registro o Identidad

8FFR20-00223-001 CSIRT ADVIERTE DE 2 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00223-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de febrero de 2020
Última revisión	20 de febrero de 2020

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 del Banco Security, 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/8ffr20-00223-001/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00223-01.pdf

8FFR20-00224-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00224-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Febrero de 2020
Última revisión	20 de Febrero de 2020

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 del 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/8ffr20-00224-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00224-01.pdf

8FFR20-00225-01 CSIRT ADVIERTE DE 6 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00225-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis portales fraudulentos asociados a tres IP que suplantan el sitio web oficial del 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/8ffr20-00225-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00225-01.pdf

8FFR20-00226-01 CSIRT ADVIERTE 6 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00226-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis portales fraudulentos asociados a tres IP que suplantan 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/8ffr20-00226-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00226-01.pdf

8FFR20-00227-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00227-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

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 del 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/8ffr20-00227-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00227-01.pdf

8FFR20-00228-01 CSIRT ADVIERTE DE PÁGINA BANCARIA FRAUDULENTA

Alerta de seguridad informática	8FFR20-00228-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Febrero de 2020
Última revisión	22 de Febrero de 2020

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 del 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/8ffr20-00228-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00228-01.pdf

8FFR20-00229-01 CSIRT ADVIERTE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00229-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2020
Última revisión	25 de Febrero de 2020

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 del 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/8ffr20-00229-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00229-01.pdf

Phishing

8FPH20-00116-01 CSIRT INFORMA PHISHING DE AUMENTO EN EL CUPO DE TARJETA BANCARIA

Alerta de seguridad informática	8FPH20-00116-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Febrero de 2020
Última revisión	20 de Febrero de 2020

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 Edwards del Banco de Chile.

El atacante utiliza un mensaje indicando que revise si tiene un aumento de cupo en su tarjeta y/o línea de crédito. Esta promoción tiene una duración desde el 01 hasta el 29 de Febrero de 2020. Los estafadores disponibilizan un enlace que al seleccionarlo, la víctima es direccionada a un sitio semejante al del Banco de Chile.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00116-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00116-01.pdf

8FPH20-00117-01 CSIRT INFORMA DE PHISHING BANCARIO POR ACTUALIZACIÓN DE SEGURIDAD

Alerta de seguridad informática	8FPH20-00117-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Scotiabank.

El mensaje informa a la víctima que el banco realizó una actualización de nuevas políticas de protección de datos y seguridad, arrojando un error en la integración de la cuenta entre los bancos BBVA y Banco Scotiabank. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo. Al seleccionar el vínculo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00117-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00117-01.pdf

8FPH20-00118-01 CSIRT ADVIERTE DE PHISHING DE CUENTA SUSPENDIDA

Alerta de seguridad informática	8FPH20-00118-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa que existe un error en el sistema que se define como cuenta suspendida, ya que no ha realizado el proceso de verificación de identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que al ingresar podrá reestablecer el acceso a la cuenta o de lo contrario su servicio de internet quedará bloqueado y tendrá que acudir a la sucursal. Al seleccionar el vínculo es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00118-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00118-01.pdf

8FPH20-00119-01 CSIRT ADVIERTE PHISHING DE CUENTA SUSPENDIDA

Alerta de seguridad informática	8FPH20-00119-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Febrero de 2020
Última revisión	24 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa que la cuenta se encuentra suspendida al no realizar el proceso de verificación de identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que al ingresar podrá reestablecer el acceso a la cuenta o de lo contrario su servicio de internet quedará bloqueado y tendrá que acudir a la sucursal para desbloquear la cuenta. Al seleccionar el vínculo es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00119-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00119-01.pdf

8FPH20-00120-01 CSIRT ADVIERTE PHISHING CON MENSAJES DE DIVERSOS CONTENIDOS BANCARIOS

Alerta de seguridad informática	8FPH20-00120-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2020
Última revisión	25 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Scotiabank. El atacante envía mensaje de diversos contenidos, por ejemplo:

- Existe una operación irregular y que debe verificar
- Que la cuenta se encuentra suspendida por no realizar el pago de los impuestos
- Que se ha realizado un descuento de $321.00 pesos de su cuenta automáticamente

De esa forma intenta persuadir al usuario que seleccione el enlace, al hacerlo, la víctima es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00120-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00120-01.pdf

Vulnerabilidades

9VSA20-00145-01 CSIRT COMPARTE ACTUALIZACIÓN PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA20-00145-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Febrero de 2020
Última revisión	21 de Febrero de 2020

Vulnerabilidad

CVE-2020-6383
CVE-2020-6384
CVE-2020-6386

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Google, referente a múltiples vulnerabilidades que afectan a su explorador Google Chrome, las cuales de ser explotadas, permitirían a un atacante realizar la ejecución arbitraria de código sobre el sistema afectado y hasta comprometerle completamente. Este informe incluye la respectiva mitigación.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00145-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00145-01.pdf

9VSA20-00146-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PYYAML DE PYTHON

Alerta de seguridad informática	9VSA20-00146-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de febrero de 2020
Última revisión	24 de febrero de 2020

Vulnerabilidad
CVE-2019-20477
Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de múltiples fuentes, referente a una vulnerabilidad que afecta al componente PyYAML de Python, la cual de ser explotada permitiría a un atacante obtener acceso a funciones restringidas. Este informe incluye la respectiva mitigación.
Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00146-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00146-01.pdf

9VSA20-00147-01 CSIRT COMPARTE ACTUALIZACIÓN PARA GOOGLE CHROME

Alerta de seguridad informática	9VSA20-00147-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Febrero de 2020
Última revisión	26 de Febrero de 2020

Vulnerabilidad
CVE-2020-6407
CVE-2020-6418
Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Google, referente a dos vulnerabilidades que afectan a su explorador web Google Chrome, las cuales de ser explotadas permitirían a un atacante gatillar errores en la memoria y comprometer completamente al sistema afectado.
Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00147-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00147-01.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
192.241.237.68	Port Scan
162.243.135.237	Port Scan
42.229.97.99	DDoS
101.81.249.211	DDoS
223.98.188.138	DDoS
114.234.104.54	DDoS
110.253.227.250	DDoS
125.70.48.203	DDoS
112.28.174.188	DDoS
118.114.98.220	DDoS
27.23.179.128	DDoS
119.134.45.146	DDoS
104.194.10.30	Port Scan
175.183.64.180	Port Scan
192.241.220.219	Port Scan
203.151.101.39	Port Scan
212.58.103.200	Port Scan
216.170.126.116	Port Scan
223.146.37.224	Port Scan
36.228.26.89	Port Scan
45.142.195.5	Port Scan
51.159.35.140	Port Scan
192.241.235.199	Port Scan
192.241.214.87	Port Scan
221.139.104.121	Port Scan
132.248.30.249	Port Scan
192.241.238.110	Port Scan
165.22.220.251	Phishing
134.209.156.250	Phishing
68.183.95.33	Phishing
165.22.220.239	Phishing
89.248.168.226	Port Scan

142.93.209.131	Phishing
162.243.133.18	Port Scan
192.241.222.43	Port Scan
192.241.225.184	Port Scan
1.246.222.228	Port Scan
82.185.94.187	Port Scan
93.149.167.72	Port Scan
79.101.58.39	Port Scan
74.80.24.8	Port Scan
162.243.132.179	Port Scan
163.172.74.153	Port Scan
51.68.12.140	Port Scan
70.39.117.18	Port Scan
47.244.77.134	Port Scan
114.35.97.32	Port Scan
88.34.126.169	Port Scan
201.236.143.243	Bot
212.77.130.65	Bot
103.234.27.106	Bot
43.229.95.171	Bot
171.100.2.154	Bot
37.26.136.181	Bot
81.16.244.94	Bot
103.106.241.33	Bot
49.236.212.30	Bot
114.134.92.134	Bot
185.129.212.41	Bot
103.63.24.155	Bot
176.110.121.90	Bot
31.179.192.214	Bot
187.189.82.93	Bot
192.241.234.107	Port Scan
192.241.235.199	Port Scan
54.180.102.65	Port Scan
79.122.53.88	Port Scan
92.246.84.200	Port Scan
77.247.108.21	Port Scan
139.99.125.193	Port Scan
51.89.2.211	Port Scan
84.234.96.71	Port Scan
77.247.110.167	Port Scan

162.243.133.185	Port Scan
165.22.216.99	Port Scan
192.241.237.45	Port Scan
192.241.234.6	Port Scan
162.243.136.28	Port Scan
193.137.124.194	Port Scan
104.219.248.48	Phishing
130.193.89.178	Phishing
192.241.218.70	Port Scan
104.243.37.234	Port Scan
139.99.125.191	Port Scan
162.243.132.27	Port Scan
192.241.226.66	Port Scan
84.234.96.71	DDoS
192.241.214.99	Port Scan
192.241.215.51	Port Scan
27.123.3.250	Port Scan
162.243.133.173	Port Scan
162.243.134.16	Port Scan
162.243.134.144	Port Scan
192.3.2.29	Port Scan
192.241.216.197	Port Scan
192.241.227.94	Port Scan
192.241.231.49	Port Scan
45.148.10.194	Port Scan
192.241.238.137	Port Scan
162.243.133.202	Port Scan
162.243.135.191	Port Scan
192.241.239.195	Port Scan
51.91.192.146	Port Scan
45.143.220.213	Port Scan
118.24.159.78	Port Scan
162.243.132.243	Port Scan
89.248.168.157	Port Scan
192.241.207.118	Port Scan
198.199.101.103	Hacking
103.3.65.10	Malware
110.49.60.66	Malware
103.140.151.7	Port Scan
122.141.236.246	Hacking
51.159.35.138	Hacking

176.113.115.252	Hacking
192.241.207.110	Hacking
192.241.218.175	Hacking
192.241.213.87	Port Scan
162.243.136.70	Port Scan
162.243.134.244	Port Scan
162.243.132.88	Port Scan
192.241.238.24	Port Scan
192.241.216.128	Port Scan
162.243.134.180	Port Scan
162.243.135.51	Port Scan
192.241.235.69	Port Scan
192.241.208.85	Port Scan
162.243.131.68	Port Scan
192.241.223.187	Port Scan
192.241.235.25	Port Scan
37.187.134.193	Port Scan
162.243.132.151	Port Scan
192.241.218.22	Port Scan
192.241.233.117	Port Scan
191.5.0.106	Port Scan
58.182.132.254	Port Scan
188.25.173.140	Port Scan
192.241.238.206	Port Scan
185.172.110.163	Port Scan
82.76.188.14	Port Scan
88.49.238.245	Port Scan
139.59.211.245	Port Scan
163.172.43.33	Port Scan
192.241.208.127	Port Scan
49.235.162.224	Hacking
49.235.118.170	Hacking
119.29.132.240	Hacking
58.244.255.45	Hacking
94.191.86.50	Hacking
122.51.182.253	Hacking
222.185.234.10	Hacking
106.13.37.56	Hacking
36.110.58.52	Hacking
192.241.208.229	Hacking
172.105.216.159	DDoS

162.243.135.61	Port Scan
192.241.219.165	Port Scan
192.241.239.50	Port Scan
193.70.65.248	Port Scan
51.178.78.152	Port Scan
192.241.229.63	Port Scan
162.243.134.77	Port Scan
162.243.134.207	Port Scan
192.241.217.164	Port Scan
192.241.221.172	Port Scan
03.94.103.222	Port Scan
162.243.133.160	Port Scan
51.178.78.153	Port Scan
51.178.78.154	Port Scan
192.241.211.136	Port Scan
45.143.220.141	Port Scan
82.196.5.139	Port Scan
185.81.154.7	Port Scan
192.241.214.201	Port Scan
162.243.134.136	Port Scan
192.241.223.105	Port Scan
194.180.224.13	Port Scan
192.241.224.91	Port Scan
192.241.239.202	Port Scan
67.229.243.85	Port Scan
31.192.111.233	Hacking
77.247.110.91	Port Scan
77.247.110.92	Port Scan
104.254.92.59	Port Scan
86.57.236.141	Port Scan
1.55.142.68	Port Scan
192.241.219.43	Port Scan
103.79.141.134	Port Scan
162.243.132.60	Port Scan
162.243.132.53	Port Scan
162.243.133.194	Port Scan
162.243.134.59	Port Scan
162.243.134.119	Port Scan
192.241.215.158	Port Scan
192.241.220.57	Port Scan
194.61.27.241	Port Scan

79.124.62.53	Port Scan
148.70.163.11	Hacking
49.232.144.115	Hacking
58.87.121.46	Hacking
139.199.39.56	Hacking
49.234.94.51	Hacking
111.67.194.87	Hacking
106.54.132.65	Hacking
118.89.49.178	Hacking
139.199.74.166	Hacking
118.24.97.147	Hacking
193.112.9.107	Hacking
118.25.134.204	Hacking

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: 2020.03.05 15:32:03 -03'00'