13BCS-00028-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 15 de Noviembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 07 y el miércoles 13 de Noviembre.

Falsificación de Registro o Identidad

8FFR-00105-001 CSIRT ADVIERTE DE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00105-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Noviembre de 2019
Última revisión	07 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-00105-001/

https://www.csirt.gob.cl/media/2019/11/8FFR-00105-001.pdf

8FFR-00106-001 CSIRT ADVIERTE DE CUATRO PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00106-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Noviembre de 2019
Última revisión	10 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 4 portales fraudulentos asociado 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-00106-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00106-001.pdf

8FFR-00107-001 CSIRT ADVIERTE DE NUEVO SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00107-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Noviembre de 2019
Última revisión	11 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-00107-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00107-001.docx.pdf

8FFR-00108-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00108-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2019
Última revisión	12 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 del servicio y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00108-001-2/
https://www.csirt.gob.cl/media/2019/11/8FFR-00108-001.docx.pdf

8FFR-00109-001 CSIRT ADVIERTE SOBRE PORTAL FRAUDULENTO BANCARIO PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00109-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2019
Última revisión	13 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-00109-001/
https://www.csirt.gob.cl/media/2019/11/8FFR-00109-001.docx.pdf

8FPH-00072-001 CSIRT ADVIERTE DE PHISHING ASOCIADO A COMPAÑÍA DE SERVICIOS ELECTRÓNICOS

Alerta de seguridad informática	8FPH-00072-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Noviembre de 2019
Última revisión	07 de Noviembre 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 de la compañía de Amazon.

El correo indica que existe un problema con la cuenta de acceso y el usuario debe actualizar sus datos de la cuenta dentro de las 24 horas siguientes, de lo contrario se desactivará la cuenta de forma permanente. Los estafadores disponibilizan un enlace para actualizar la cuenta, exponiéndolos al robo de sus credenciales y datos de la tarjeta crédito desde un sitio semejante al de Amazon.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00072-001/
https://www.csirt.gob.cl/media/2019/11/8FPH-00072-001.pdf

8FPH-00073-001 CSIRT ADVIERTE DE PHISHING EN CORREO DE ACTUALIZACIÓN DE DATOS BANCARIOS

Alerta de seguridad informática	8FPH-00073-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Noviembre de 2019
Última revisión	12 de Noviembre 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 Scotiabank. El correo informa a los clientes que, producto de la fusión de los bancos Scotiabank y BBVA, es necesario actualizar la cuenta en un período máximo de 24 horas, de lo contrario, esta sería bloqueada. Los estafadores disponibilizan un enlace para actualizar la cuenta, exponiendo a los usuarios al robo de sus credenciales desde un sitio semejante al de Scotiabank.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00073-001/
https://www.csirt.gob.cl/media/2019/11/8FPH-00073-001.pdf

8FPH-00074-001 CSIRT INFORMA SOBRE CAMPAÑA DE PHISHING CON DISTINTOS MENSAJES

Alerta de seguridad informática	8FPH-00074-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2019
Última revisión	13 de Noviembre 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 de Chile. El atacante utiliza varios mensajes en el cuerpo del correo para persuadir al usuario para que seleccione un enlace, siendo direccionado a un sitio semejante al del banco. De esta forma los estafadores podrían capturar las credenciales bancarias de los clientes. A continuación se detallan algunos de los mensajes con los que se intenta engañar a los usuarios.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00074-001/
https://www.csirt.gob.cl/media/2019/11/8FPH-00074-001.pdf

Alertas de Malware

2CMV-00039-001 CSIRT ADVIERTE DE MALWARE EN CORREO DE ACTUALIZACIÓN DE DATOS BANCARIOS

Alerta de seguridad informática	2CMV-00039-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Noviembre de 2019
Última revisión	11 de Noviembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado una campaña de phishing con malware asociado, a través de un correo electrónico que suplanta al Banco ScotiaBank. Los estafadores buscan engañar a los usuarios enviando un anuncio que tiene relación con la fusión entre los Bancos BBVA y Scotiabank, advirtiéndoles que producto de este proceso, el usuario debe actualizar sus datos, lo que también es necesario para brindar seguridad a la misma.

A la víctima se le disponibiliza un enlace para realizar la actualización de sus datos. Al seleccionar el hipervínculo, la personas es direccionado a otro sitio hasta descargar el archivo malicioso.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00039-001/
https://www.csirt.gob.cl/media/2019/11/2CMV-00039-001.docx.pdf

Vulnerabilidades

9VSA-00083-001 CSIRT INFORMA DE VULNERABILIDAD EN LIBARCHIVE Y MITIGACIÓN

Alerta de seguridad informática	9VSA-00083-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	08 de Noviembre de 2019
Última revisión	08 de Noviembre de 2019

Vulnerabilidad

CVE-2019-18408

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por diferentes fuentes, referente a una vulnerabilidad en la biblioteca de compresión 'libarchive', utilizada en múltiples distribuciones de Linux, FreeBSD y NetBSD, la cual permite generar ataques de tipo ejecución de código remoto. También se comparte su respectiva forma de mitigarla.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00083-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00083-001.docx.pdf

9VSA-00084-001 CSIRT COMPARTE ACTUALIZACIONES PARA CISCO

Alerta de seguridad informática	9VSA-00084-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de noviembre de 2019
Última revisión	11 de noviembre de 2019

Vulnerabilidad

CVE-2019-15270
CVE-2019-15973
CVE-2019-15974
CVE-2019-15959
CVE-2019-15967
CVE-2019-15960
CVE-2019-15969
CVE-2019-15958
CVE-2019-15957
CVE-2019-15283
CVE-2019-15284
CVE-2019-15285
CVE-2019-15286
CVE-2019-15287
CVE-2019-15276

CVE-2019-15271
CVE-2019-15956
CVE-2019-15289
CVE-2019-15288

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00084-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00084-001.pdf

9VSA-00085-001 CSIRT COMPARTE ACTUALIZACIONES DE NOVIEMBRE ENTREGADAS POR MICROSOFT

Alerta de seguridad informática	9VSA-00085-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de noviembre de 2019
Última revisión	13 de noviembre de 2019

Vulnerabilidad

Informados en el boletín de octubre

ADV190024	CVE-2019-1409	CVE-2019-1442
CVE-2018-12207	CVE-2019-1411	CVE-2019-1443
CVE-2019-11135	CVE-2019-1412	CVE-2019-1445
CVE-2019-1324	CVE-2019-1418	CVE-2019-1446
CVE-2019-1370	CVE-2019-1432	CVE-2019-1447
CVE-2019-1374	CVE-2019-1436	CVE-2019-1448
CVE-2019-1381	CVE-2019-1439	CVE-2019-1449
CVE-2019-1402	CVE-2019-1440	CVE-2019-1457

Informados adicionalmente

CVE-2019-0712	CVE-2019-1394	CVE-2019-1423
CVE-2019-0721	CVE-2019-1395	CVE-2019-1424
CVE-2019-1234	CVE-2019-1396	CVE-2019-1425
CVE-2019-1309	CVE-2019-1397	CVE-2019-1426
CVE-2019-1310	CVE-2019-1398	CVE-2019-1427
CVE-2019-1373	CVE-2019-1399	CVE-2019-1428
CVE-2019-1379	CVE-2019-1405	CVE-2019-1429
CVE-2019-1380	CVE-2019-1406	CVE-2019-1430
CVE-2019-1382	CVE-2019-1407	CVE-2019-1433
CVE-2019-1383	CVE-2019-1408	CVE-2019-1434
CVE-2019-1384	CVE-2019-1413	CVE-2019-1435
CVE-2019-1385	CVE-2019-1414	CVE-2019-1437
CVE-2019-1388	CVE-2019-1415	CVE-2019-1438
CVE-2019-1389	CVE-2019-1416	CVE-2019-1441
CVE-2019-1390	CVE-2019-1417	CVE-2019-1454

CVE-2019-1391	CVE-2019-1419	CVE-2019-1456
CVE-2019-1392	CVE-2019-1420	
CVE-2019-1393	CVE-2019-1422	

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 noviembre del 2019, publicando 2 avisos y actualizaciones para 74 vulnerabilidades en sus sotwares, 13 de ellos, clasificados como críticos.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00085-001/
https://www.csirt.gob.cl/media/2019/11/9VSA-00085-001.docx.pdf

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	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de noviembre de 2019
Última revisión	14 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

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
185.10.99.14	Hacking
162.241.134.70	Hacking
124.65.18.102	Port Scan
159.203.193.251	Port Scan
128.14.181.142	Port Scan
192.99.169.110	Port Scan
83.97.20.19	Port Scan
43.255.84.13	Port Scan
104.143.83.242	Port Scan
92.63.194.17	Port Scan
185.175.93.45	Port Scan
185.254.68.170	Port Scan
185.153.196.191	Port Scan
167.172.132.231	Port Scan
92.119.160.38	Port Scan
37.49.230.9	Port Scan
77.247.110.244	Port Scan
159.203.197.155	Port Scan
159.89.165.2	Port Scan
92.119.160.145	Port Scan
185.254.68.172	Port Scan
185.254.68.171	Port Scan
77.227.105.140	Port Scan
144.91.91.116	Port Scan
103.253.2.132	Port Scan
118.24.49.139	Hacking
51.77.83.253	Port Scan
139.99.0.25	Port Scan
159.203.193.38	Port Scan
139.99.128.97	Port Scan
14.102.254.230	Port Scan
51.159.57.72	Port Scan
218.205.57.15	Port Scan
218.205.57.16	Port Scan
117.52.89.197	Phishing
159.153.78.110	Port Scan

159.153.78.109	Port Scan
172.105.4.63	Port Scan
5.9.16.100	Port Scan
58.225.75.147	Port Scan
185.175.93.37	Port Scan
185.153.197.5	Port Scan
193.32.161.113	Port Scan
193.200.164.135	Port Scan
185.200.118.36	Port Scan
176.46.120.196	Port Scan
185.176.221.41	Port Scan
185.40.4.23	Port Scan
198.251.81.54	Port Scan
103.79.143.102	Port Scan
139.162.14.167	Hacking
132.232.155.232	Hacking
158.69.58.45	Port Scan
172.105.119.149	Port Scan
217.138.202.2	Port Scan
83.97.20.46	Port Scan
96.126.100.87	Port Scan
120.224.187.89	Port Scan
138.68.212.139	Port Scan
159.89.165.2	Port Scan
122.114.254.38	Hacking
109.70.100.21	DDoS
162.247.74.202	DDoS
77.247.181.165	DDoS
185.156.73.49	Port Scan
185.156.73.42	Port Scan
185.156.73.7	Port Scan
185.156.73.14	Port Scan
185.156.73.11	Port Scan
185.156.73.45	Port Scan
185.156.73.17	Port Scan
185.156.73.25	Port Scan
185.156.73.3	Port Scan
185.156.73.27	Port Scan
185.156.73.34	Port Scan
185.156.73.21	Port Scan
185.156.73.38	Port Scan
185.156.73.31	Port Scan

185.156.73.52	Port Scan
103.133.107.211	Port Scan
103.207.38.153	Port Scan
89.248.174.216	Port Scan
144.217.169.90	Port Scan
220.130.73.44	Port Scan
185.216.140.7	Port Scan
185.175.93.27	Port Scan
185.176.27.54	Port Scan
77.247.108.52	Port Scan
51.91.201.54	Port Scan
37.49.230.18	Port Scan
144.48.243.204	Port Scan
220.189.199.38	Port Scan
159.203.193.54	Port Scan
45.143.220.40	Port Scan
159.203.197.154	Port Scan
185.200.118.70	Port Scan
173.212.195.112	Port Scan
159.203.197.0	Port Scan
177.75.21.139	Port Scan
62.210.84.26	Port Scan
46.36.39.97	Port Scan
157.245.242.71	Port Scan
112.175.184.69	Port Scan
213.109.220.204	Port Scan
199.195.250.111	Port Scan
54.36.160.211	Port Scan
45.10.88.55	Port Scan
77.247.110.46	Port Scan
87.98.219.59	Port Scan
45.67.15.140	Port Scan
185.36.81.249	Port Scan
185.53.160.165	Port Scan
159.203.197.2	Port Scan
163.47.87.28	Port Scan
92.63.194.115	Port Scan
37.49.230.23	Port Scan
110.77.246.7	Port Scan
5.83.161.240	Port Scan
45.236.8.5	Port Scan
159.203.197.7	Port Scan

62.138.6.197	Port Scan
37.49.231.115	Port Scan
163.30.164.6	Port Scan
185.53.91.65	Port Scan
94.102.53.10	Port Scan
92.63.194.55	Port Scan
158.69.123.115	Port Scan
13.94.247.106	Port Scan
139.59.60.161	Phishing
77.247.109.38	Port Scan
93.192.16.253	Port Scan
104.243.37.48	Port Scan
95.217.255.75	DDoS
159.203.193.51	Port Scan

URL	Motivo
https[://]estadocl[.]logosbanking[.]com/index_2[.]html	Phishing
https[://]6y3zelqlstbiutogfjgf9q-on[.]drv[.]tw/bncstado1/index_2[.]html	Phishing
https[://]www[.]scotiaseguridad[.]site/site/persona/acesso[.]php	Phishing
https[://]www[.]scotiafreeemail[.]com/site/choose-type[.]php	Phishing
https[://]bnchilee[.]com/persona/login/	Phishing
https[://]www[.]technostoremm[.]com	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

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.

- Abraham Ermann - https://www.linkedin.com/in/aermann/

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: 2019.11.15 15:41:55 -03'00'