13BCS-00018-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 15 de Agosto de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 08 y el miércoles 14 de Agosto.

Noticias

Publicado 10 agosto, 2019

Datos de Pasajeros de Aerolínea Neozelandesa Expuestos Por Incidente de Ciberseguridad

El incidente afectó a la línea aérea Air New Zeland, en el que según expertos, podrían haber quedado expuestos miles de datos de 3% de pasajeros inscritos en el sistema Airpoints, revelando nombres, direcciones, fechas de nacimientos y, posiblemente, detalles de pasaportes.

Enlace:

https://www.csirt.gob.cl/noticias/miles-de-datos-de-aerolinea-neozelandesa-expuesto-por-incidente/

Publicado 14 agosto, 2019

Reporte de la ONU destaca el uso de ingeniería social en ataque a la banca chilena por parte de grupos Norcoreanos en 2018

El informe, al que tuvo acceso la agencia noticiosa The Associated Press, indica que el objetivo de los ciberataques sería el financiamiento de armas de destrucción masiva. Chile figura tercero entre los 17 países afectados, con 2 ataques de un total de 35 perpetrados por Norcorea a nivel global.

Enlace:

https://www.csirt.gob.cl/noticias/reporte-de-la-onu-destaca-el-uso-de-ingenieria-social-en-ataque-a-la-banca-chilena-por-parte-de-grupos-norcoreanos-en-2018/

Falsificación de Registro o Identidad

8FFR-00011-001 CSIRT INFORMA SOBRE DOMINIOS FALSOS BANCARIOS

Alerta de seguridad informática	8FFR-00011-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto de 2019

Resumen

El El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado un dominio fraudulento que no pertenecía al Banco de Chile, el que sospecha sería utilizado para suplantar el sitio web oficial del BANCODECHILE.CL con el objetivo de realizar algún fraude bancario. El CSIRT informó oportunamente a la entidad bancaria con el objetivo de desechar cualquier tipo de relación de propiedad u otra con el sitio sospechoso, así como para coordinar una respuesta adecuada para contener el incidente.

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00011-001-1.pdf
https://www.csirt.gob.cl/alertas/8ffr-00011-001-csirt-informa-sobre-dominios-falsos-bancarios/

8FFR-00012-001 CSIRT ADVIERTE DE INTENTO DE SUPLANTANCIÓN DE SITIO BANCARIO

Alerta de seguridad informática	8FFR-00012-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del BANCOESTADO.CL el que podría servir para robar credenciales de usuarios del banco.

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/media/2019/08/8FFR-00012-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00012-001-csirt-advierte-de-intento-de-suplantancion-de-sitio-bancario/

8FFR-00011-002 CSIRT ACTUALIZA INFORMA SOBRE DOMINIOS FALSOS BANCARIOS

Alerta de seguridad informática	8FFR-00011-002
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con el apoyo del SOP (SOC del Ministerio de Obras Públicas) actualizan la información sobre un dominio fraudulento que, se sospecha, sería utilizado para suplantar el sitio web oficial del BANCODECHILE.CL con el objetivo de perjudicar a usuarios, clientes y al banco aludido.

El CSIRT informó oportunamente a la entidad bancaria con el objetivo de desechar cualquier tipo de relación de propiedad u otra con el sitio sospechoso, así como para coordinar una respuesta adecuada para contener el incidente.

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00011-002.pdf

https://www.csirt.gob.cl/alertas/8ffr-00011-002-csirt-actualiza-informa-sobre-dominios-falsos-bancarios/

8FFR-00013-001 CSIRT ADVIERTE DE DOMINIOS SOSPECHOSOS PARA USO DE SUPLANTACIÓN BANCARIA

Alerta de seguridad informática	8FFR-00013-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado una serie de dominios que se sospecha podrían ser utilizados para suplantar el sitio web oficial del bancoestado.cl con el objetivo de perjudicar a usuarios, clientes y al banco aludido.

El CSIRT informó oportunamente a la entidad bancaria con el objetivo de desechar cualquier tipo de relación de propiedad u otra con el sitio sospechoso, así como para coordinar una respuesta adecuada para contener el incidente.

Actualmente los sitios señalados están inactivos, pero pueden ser activados en cualquier momento con los fines antes señalados.

Enlace:

https://www.csirt.gob.cl/media/2019/08/8FFR-00013-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00013-001-csirt-advierte-de-dominios-sospechosos-para-uso-de-suplantacion-bancaria/

8FFR-00014-001 CSIRT ADVIERTE DE SITIO QUE SUPLANTA A WEB BANCARIA

Alerta de seguridad informática	8FFR-00014-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Agosto de 2019
Última revisión	10 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del bancoestado.cl 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/media/2019/08/8FFR-00014-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00014-001/

8FFR-00015-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO QUE SUPLANTA A WEB BANCARIA

Alerta de seguridad informática	8FFR-00015-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del bancoedwards.cl 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/media/2019/08/8FFR-00015-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00015-001-csirt-advierte-de-sitio-fraudulento-que-suplanta-a-web-bancaria/

8FFR-00016-001 CSIRT ADVIERTE DE DOMINIO QUE INTENTA SUPLANTAR A SITIO BANCARIO

Alerta de seguridad informática	8FFR-00016-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del bancobci.cl 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/media/2019/08/8FFR-00016-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00016-001-csirt-advierte-de-dominio-que-intenta-suplantar-a-sitio-bancario/

8FFR-00017-001 CSIRT ADVIERTE DE WEB SOSPECHOSA DE SUPLANTAR SITIO BANCARIO

Alerta de seguridad informática	8FFR-00017-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del bancoedwards.cl 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/media/2019/08/8FFR-00017-001.pdf

https://www.csirt.gob.cl/alertas/8ffr-00017-001-csirt-advierte-de-web-sospechosa-que-podria-ser-utilizada-para-fraude-bancario/

Alertas de Phishing

8FPH-00055-001 CSIRT ADVIERTE DE PHISHING BANCARIO ASOCIADO A MENSAJE DE ACTUALIZACIÓN DE DISPOSITIVO DIGIPASS

Alerta de seguridad informática	8FPH-00055-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 de Agosto 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 de Chile, para que sincronicen su dispositivo DigiPass ya que existe un error, el cual se solucionaría con la sincronización, indicando que esta acción es "obligatoria", de lo contrario la cuenta podría ser bloqueada por temas de seguridad. Si el usuario ingresa al enlace se expone a que el atacante robe sus credenciales desde un sitio semejante al del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/08/8FPH-00055-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00055-001-csirt-advierte-de-phishing-bancario-asociado-a-mensaje-de-actualizacion-de-dispositivo-digipass/

Vulnerabilidades

9VSA-00031-001 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIONES DE CISCO

Alerta de seguridad informática	9VSA-00031-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2019
Última revisión	8 de agosto de 2019

Vulnerabilidad

CVE-2019-1912	CVE-2019-1945
CVE-2019-1960	CVE-2019-1954
CVE-2019-1913	CVE-2019-1955
CVE-2019-1973	CVE-2019-1934
CVE-2019-1914	CVE-2019-1949
CVE-2019-1946	CVE-2019-1910
CVE-2019-1941	CVE-2019-1957
CVE-2019-1951	CVE-2019-1918
CVE-2019-1944	CVE-2019-1970
CVE-2019-1956	CVE-2019-1895

CVE-2019-1958
CVE-2019-1924
CVE-2019-1952
CVE-2019-1925
CVE-2019-1971
CVE-2019-1926
CVE-2019-1961
CVE-2019-1927
CVE-2019-1972
CVE-2019-1928
CVE-2019-1953
CVE-2019-1929
CVE-2019-1959

Resumen

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

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00031-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00031-001/

9VSA-00032-001 CSIRT COMPARTE ACTUALIZACIONES DE FORTNINET PARA VARIOS DE SUS PRODUCTOS

Alerta de seguridad informática	9VSA-00032-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Agosto de 2019
Última revisión	11 de Agosto de 2019

Vulnerabilidad

CVE-2018-13379
CVE-2018-13380
CVE-2018-13381
CVE-2018-13382
CVE-2018-13383

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por FORTINET referente vulnerabilidades que afectan a varios de sus productos, así como las actualizaciones asociadas liberadas por el proveedor.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00032-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00032-001-csirt-comparte-actualizaciones-de-fortninet-para-varios-de-sus-productos/

9VSA-00033-001 CSIRT COMPARTE INFORMACIÓN SOBRE VULNERABILIDADES Y LOS RESPECTIVOS PARCHES EN PRODUCTOS DE MICROSOFT

Alerta de seguridad informática	9VSA-00033-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Agosto de 2019
Última revisión	13 de Agosto de 2019

Vulnerabilidad

CVE-2019-1181
CVE-2019-1182
CVE-2019-1222
CVE-2019-1226

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft este martes 13 de agosto, referente a actualizaciones de seguridad para hacer frente a vulnerabilidades calificadas como críticas y que pueden permitir el control remoto de un atacante sin requerir información.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00033-001.pdf
https://www.csirt.gob.cl/alertas/9vsa-00033-001-csirt-comparte-informacion-sobre-vulnerabilidades-y-los-respectivos-parches-en-productos-de-microsoft/

9VSA-00034-001 CSIRT COMPARTE ACTUALIZACIONES DE MICROSOFT

Alerta de seguridad informática	9VSA-00034-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Agosto de 2019
Última revisión	13 de Agosto de 2019

Vulnerabilidad

ADV190014	CVE-2019-1146
CVE-2019-1157	CVE-2019-1172
CVE-2019-1205	CVE-2019-1227
CVE-2019-1030	CVE-2019-1147
CVE-2019-1158	CVE-2019-1181
CVE-2019-1218	CVE-2019-1228
CVE-2019-1078	CVE-2019-1148
CVE-2019-1161	CVE-2019-1182
CVE-2019-1224	CVE-2019-9511
CVE-2019-1143	CVE-2019-1149
CVE-2019-1171	CVE-2019-1199
CVE-2019-1225	CVE-2019-9512

CVE-2019-1151
CVE-2019-1200
CVE-2019-9513
CVE-2019-1153
CVE-2019-1201
CVE-2019-9514
CVE-2019-1154
CVE-2019-1202
CVE-2019-9518
CVE-2019-1155
CVE-2019-1203
CVE-2019-1156
CVE-2019-1204

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a actualizaciones de seguridad para hacer frente a vulnerabilidades que afectan a varios de sus productos.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00034-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00034-001-csirt-comparte-actualizaciones-de-microsoft/

9VSA-00034-001 CSIRT COMPARTE ACTUALIZACIONES DE MICROSOFT

Alerta de seguridad informática	9VSA-00034-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 de Agosto de 2019

Vulnerabilidad

CVE-2019-8062
CVE-2019-8063
CVE-2019-7870
CVE-2019-7957
CVE-2019-7931
CVE-2019-7958
CVE-2019-7961
CVE-2019-7959

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Adobe referente vulnerabilidades detectadas en varios de sus productos y sus respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00035-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00035-001-csirt-comparte-informacion-entregada-por-adobe-sobre-vulnerabilidades-y-parches-en-sus-productos/

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante la pasada semana 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:

IP's	Causa Asociada
178[.]159[.]36[.]236	Scan
46[.]105[.]234[.]11	Hacking
80.211.245.229	Scan
212[.]129[.]1[.]251	Scan
185[.]53[.]88[.]25	Scan
81[.]177[.]143[.]31	Scan
216.245.193.238	Hacking
42.231.162.204	Hacking
162[.]243[.]134[.]70	Scan
77[.]247[.]110[.]76	Scan
194[.]32[.]71[.]4	Scan
171[.]83[.]40[.]212	Scan
147.135.122.155	Scan
111[.]19[.]230[.]103	Scan
77.247.110.234	Hacking
62[.]210[.]172[.]36	Scan
77.247.110.226	Scan
42.231.162.207	Hacking
42.231.162.196	Hacking
60[.]191[.]0[.]244	Scan
60[.]191[.]23[.]59	Scan

URL's Bloqueadas	Causas Asociadas
hxxps[:]//upgrademail4[.]wixsite[.]com/mysite	Phishing
hxxps[:]//viveropaztrana-urban[.]net/	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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.15 21:06:30 -04'00'