13BCS-00019-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 22 de Agosto de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 15 y el miércoles 21 de Agosto.

Noticias

Publicado 18 agosto, 2019

Banco Central Europeo cierra sitio web tras brecha de seguridad

La información fue entregada por la propia entidad afectada, indicando que el quiebre de las medidas de seguridad afectó específicamente al Diccionario Integrado de Informes, conocido como reporte BIRD, el cual es particularmente sensible, ya que provee a la industria bancaria con detalles para la producción de informes estadísticos y de supervisión.

Enlace:

https://www.csirt.gob.cl/noticias/banco-central-europeo-cierra-sitio-web-tras-brecha-de-seguridad/

Publicado 21 agosto, 2019

22 Localidades de Texas víctimas de un ataque coordinado de Ransomware

El ataque se inició en la mañana del 16 de agosto, lo que fue advertido por el SOC (Centro de Operaciones de Seguridad del Estado) poco antes del mediodía, activando a una serie de entidades para dar apoyo a los condados afectados. Entre ellas se cuentan el Departamento de Recursos de la Información (DIR) que lidera el proceso.

Enlace:

https://www.csirt.gob.cl/noticias/22-localidades-de-texas-victimas-de-un-ataque-coordinado-de-ransomware/

Falsificación de Registro o Identidad

8FFR-00018-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO QUE IMITA SITIO WEB BANCARIO

Alerta de seguridad informática	8FFR-00018-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Agosto de 2019
Última revisión	15 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-00018-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00018-001-csirt-advierte-de-portal-fraudulento-que-imita-sitio-web-bancario/

8FFR-00019-001 CSIRT ADVIERTE DE SITIO QUE SUPLANTA WEB BANCARIA PARA COMETER FRAUDES

Alerta de seguridad informática	8FFR-00019-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Agosto de 2019
Última revisión	15 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 bancochile.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-00019-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00019-001-csirt-advierte-de-sitio-que-suplanta-web-bancaria-para-cometer-fraudes/

8FFR-00020-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00020-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Agosto de 2019
Última revisión	19 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-00020-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00020-001-csirt-advierte-de-portal-bancario-fraudulento/

8FFR-00021-001 CSIRT ADVIERTE DE 161 SITIOS BANCARIOS FRAUDULENTOS ASOCIADAS A IP

Alerta de seguridad informática	8FFR-00021-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2019
Última revisión	20 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 161 portales fraudulentos asociados a una IP que suplantan el sitio web oficial del bancochile.cl, los 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/media/2019/08/8FFR-00021-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00021-001-csirt-advierte-de-161-sitios-bancarios-fraudulentos-asociadas-a-ip/

8FFR-00022-001 CSIRT ADVIERTE DE NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00022-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2019
Última revisión	21 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación un portal fraudulento asociado a una IP que suplanta el sitio web oficial del bancofalabella.cl, los 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/media/2019/08/8FFR-00022-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00022-001-csirt-advierte-de-nuevo-portal-bancario-fraudulento/

8FFR-00023-001 CSIRT ADVIERTE DE ACTIVACIÓN DE PORTAL FRAUDULENTO DE BANCO

Alerta de seguridad informática	8FFR-00023-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Agosto de 2019
Última revisión	21 de Agosto 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 del bancoitau.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-00023-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00023-001-csirt-advierte-de-activacion-de-portal-fraudulento-de-banco/

8FPH-00056-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH-00056-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Agosto de 2019
Última revisión	18 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración de usuarios de redes sociales, ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco BCI, notificándoles en el correo que su cuenta ha sido suspendida temporalmente ya que su correo electrónico no se encuentra registrado debidamente en la banca por internet. Por lo antes mencionado el atacante solicita ingresar al enlace indicado en el correo. Al hacerlo, el usuario ingresa 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-00056-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00056-001-csirt-advierte-de-phishing-bancario-por-suspension-de-cuenta/

8FPH-00057-001 CSIRT ADVIERTE DE PHISHING POR CUENTA BLOQUEADA Y ERROR EN REGISTRO

Alerta de seguridad informática	8FPH-00057-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2019
Última revisión	20 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 Estado, notificándoles en el correo que su cuenta ha sido bloqueada temporalmente ya que se han realizado actualizaciones en servidores de procesos bancarios y esgrimiendo que la cuenta no se encontraría registrada debidamente en la banca por internet, el atacante solicita al usuario que ingrese al enlace a través de la imagen indicada en el correo. Si el usuario ingresa al enlace este 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-00057-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00057-001/

Alertas de Adware

2CMV-00025-001 CSIRT ADVIERTE DE SITIOS DE ADWARE (PUBLICIDAD NO DESEADA)

Alerta de seguridad informática	2CMV-00025-001
Clase de alerta	Código Malicioso
Tipo de incidente	Adware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Agosto de 2019
Última revisión	20 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado sitios relacionados a anuncios publicitarios no deseados (Adware). Este ataque de ingeniería social intenta persuadir a los usuarios para que seleccionen "permitir" en el mensaje que aparece en el navegador, lo que como consecuencia multiplicará el envío de anuncios no deseados directamente al equipo del afectado. El anuncio puede ser activado al ingresar en algún sitio no confiable. El usuario será bombardeado de mensajes para ver contenidos o para descargar información. También cabe la posibilidad que un usuario haya instalado algún software gratuito que contenga un Adware, por ejemplo, a través de una "Play Store" con aplicaciones (APK), ofreciendo anuncios no deseados. Dichas aplicaciones se hacen pasa por aplicaciones legítimas especialmente centrada en juegos y fotografías.

Enlace

https://www.csirt.gob.cl/media/2019/08/2CMV-00025-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00025-001-csirt-advierte-de-sitios-de-adware-publicidad-no-deseada/

Vulnerabilidades

9VSA-00035-001 CSIRT COMPARTE INFORMACIÓN ENTREGADA POR ADOBE SOBRE VULNERABILIDADES Y PARCHES EN SUS PRODUCTOS

Alerta de seguridad informática	9VSA-00035-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	14 de 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/

9VSA-00036-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIONES EN EL NAVEGADOR FIREFOX

Alerta de seguridad informática	9VSA-00036-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Agosto de 2019
Última revisión	16 de Agosto de 2019

Vulnerabilidad

CVE-2019-11733

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Mozilla referente a una vulnerabilidad detectadas en su navegador Firefox, así como el parche necesario para subsanar el problema.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00036-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00036-001-csirt-comparte-informacion-sobre-actualizaciones-en-el-navegador-firefox/

9VSA-00038-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIÓN DE PRODUCTOS EN MICROSOFT ASOCIADO A CVE-2019-1162

Alerta de seguridad informática	9VSA-00038-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Agosto de 2019
Última revisión	18 de Agosto de 2019

Vulnerabilidad

CVE-2019-1162

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a una actualización de seguridad para hacer frente a una vulnerabilidad que afecta a Windows.

Enlace
https://www.csirt.gob.cl/media/2019/08/9VSA-00038-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00038-001-csirt-comparte-informacion-sobre-actualizacion-de-productos-en-microsoft-asociado-a-cve-2019-1161/

9VSA-00032-002 CSIRT REITERA INFORMACIÓN SOBRE ACTUALIZACIONES DE FORTNINET PARA VARIOS DE SUS PRODUCTOS

Alerta de seguridad informática	9VSA-00032-002
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	19 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, en colaboración con NIVEL4 Cybersecurity, organización que realizó diversas pruebas de concepto en torno a las vulnerabilidades que se detallan a continuación, comparte nuevamente la información entregada por FORTINET referente a una serie de vulnerabilidades que afectan a varios de sus productos, así como las actualizaciones asociadas que fueron liberadas por el proveedor. CSIRT hace un llamado a todas las entidades públicas y privadas que aún no hayan instalado los parches de seguridad, para que lo hagan a la brevedad.

Enlace
https://www.csirt.gob.cl/media/2019/08/9VSA-00032-002.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00032-001-csirt-reitera-informacion-sobre-actualizaciones-de-fortninet-para-varios-de-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
151.139.128.10	Scan
184.168.221.54	Scan
77.247.110.27	Scan

163.172.7.215	Scan
46.161.27.77	Scan
92.119.160.251	Scan
92.119.160.250	Scan
92.119.160.73	Scan
85.209.0.226	Scan
77.247.110.58	Scan
198.50.180.210	Scan
213.186.33.40	Scan
116.203.100.199	Scan
216.245.218.250	Scan
104.152.52.25	Hacking
80.82.77.212	Hacking
167.71.47.208	Hacking
37.49.224.150	Hacking
184.105.139.67	Hacking
192.173.146.34	Hacking
195.154.49.119	Hacking
185.200.118.83	Scan
51.15.146.34	Scan
85.204.124.137	Scan
71.6.232.7	Scan
162.243.151.186	Scan
163.172.35.193	Hacking
104.129.128.67	Hacking
85.128.255.199	Phishing
83.97.20.167	spam
185.200.118.45	scan
159.253.28.197	spam
147.135.124.110	spam
77.247.108.176	scan
64.71.142.226	scan
173.252.84.123	scan
78.40.112.1	scan
163.172.209.114	scan
66.220.156.52	scan
66.102.32.112	scan
27.71.195.37	scan
66.220.156.49	scan
66.220.156.48	scan

URL's Bloqueadas	Causas Asociadas
bancoestad-cl.site./imagenes/comun2009/en-linea-personas.php	Phishing
http[://]withlovestudio[.]net/wp-content/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
https://bbva.mx.accesodigital.bbva.mx.portal690.xyz/bbva.mx.banca.en.linea.personas.acceso(&7fa686506d1b18&)/home.php	Phishing
https://www.bancochile-cl[.]com/wps/26jzozngxp/dp199_persona/login_i9i1/index/loginqkiy/	Phishing
https://www.bancoestado.life/imagenes/comun2009/en-linea-personas.php	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.

- Ricardo Parra - https://www.linkedin.com/in/ricardo-parra-chavez/
- Aaron Jaramillo - https://www.linkedin.com/in/aaronje/
- Felipe Ovalle - https://www.linkedin.com/in/felipeovalle/
- Juan López - https://www.linkedin.com/in/jclopezc/
- Patricio Jofré - https://twitter.com/CasperNear
- Nivel 4 Cybersecurity - https://www.linkedin.com/company/nivel4-seguridad

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.08.22
16:52:52 -04'00'