CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Miércoles 24 de Julio del 2019

Resumen de Reportes, Alertas e Indicadores informadas por CSIRT entre el Jueves 18 y el Miércoles 24 de Julio.

Alertas de Phishing

8FPH-00047-001 CSIRT ADVIERTE DE PHISHING EN SINCRONIZACIÓN DE DIGIPASS

Características

Alerta de Seguridad Informática (8FPH-00047-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 23 de Julio de 2019 | Última revisión 23 de Julio 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 engañar a los usuarios del Banco Chile. Los correos intentan engañar a los usuarios indicando que el dispositivo digipass que posee debe ser sincronizado por internet. El mensaje intenta persuadir a la potencial víctima enfatizando que la operación es necesaria para poder ingresar a su cuenta en línea y así beneficiarse de los servicios que ofrece el banco. Para ejercer aún más presión en la decisión del usuario, el mensaje advierte al usuario que "solo tiene 48 horas para poder realizar este proceso mediante el enlace brindado, de lo contrario la cuenta será inhabilitada". De este modo, el atacante intenta de convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00047-001.pdf

8FPH-00048-001 CSIRT ADVIERTE DE PHISHING POR BLOQUEO DE CUENTA

Características

Alerta de Seguridad Informática (8FPH-00048-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio 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 engañar a los usuarios del Banco de Estado. El correo informa a las víctimas que se realizó un mantenimiento en los servicios del banco y producto de ello, se encontró un error en la cuenta del usuario. Lo anterior obligó al bloqueó de la cuenta, y la única forma de activarla nuevamente es seleccionando el enlace indicado en el correo. De este modo, el atacante intenta convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00048-001.pdf

8FPH-00049-001 CSIRT ADVIERTE DE PHISHING POR AUMENTO DE CUPO EN TARJETA DE CRÉDITO

Características

Alerta de Seguridad Informática (8FPH-00049-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio 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 engañar a los usuarios del Banco Chile. El correo informa a las víctimas que deben revisar si tienen un aumento de cupo en su tarjeta y/o línea de crédito, la cual tiene una vigencia hasta el 31 de julio del 2019. Para verificar la vigencia de la supuesta oferta, se invita al usuario a seleccionar el enlace indicado en el correo, direccionando al afectado a un sitio semejante al del banco para que entregue sus credenciales bancarias.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00049-001.pdf

Alertas de Malware

2CMV-00022-001 CSIRT ADVIERTE DE MALWARE EN FACTURA PENDIENTE

Características

Alerta de Seguridad Informática (2CMV-00022-001)
Nivel de Riesgo: Alto
Tipo: Phishing - Malware
Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con Malware, indicando que existe una copia de pago pendiente en un documento adjunto. El atacante persuade a la víctima para que descargue el documento que presuntamente proviene de Itau Corpbanca. El documento es un archivo ZIP, el que al ser ejecutado desencadena la infección.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00022-001.pdf

Vulnerabilidades

9VSA-00021-001 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIONES PARA PRODUCTOS CISCO

Características

Alerta de Seguridad Informática (9VSA-00021-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 18 de Julio de 2019 | Última revisión 18 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información liberado por Cisco que contiene actualizaciones de seguridad para abordar las vulnerabilidades en varios de sus productos. Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado o bien realizar ataques de denegación de servicio.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00021-001.pdf

9VSA-00022-001 CSIRT COMPARTE 3 ACTUALIZACIONES DE CISCO

Características

Alerta de Seguridad Informática (9VSA-00022-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 22 de Julio de 2019 | Última revisión 22 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información liberado por Cisco sobre tres actualizaciones de seguridad para abordar vulnerabilidades con clasificación alta y crítica. Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado o bien realizar ataques de denegación de servicio.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00022-001.pdf

9VSA-00023-001 CSIRT ADVIERTE SOBRE ACTUALIZACIÓN PARA VPN CORPORATIVA

Características

Alerta de Seguridad Informática (9VSA-00023-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte información sobre actualizaciones que Palo Alto Network ha publicado sobre una vulnerabilidad de severidad crítica asociada al uso de su producto de Red Privada Virtual (VPN), que podría permitir a un atacante no autenticado ejecutar un código arbitrario.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00023-001.pdf

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:

85.214.228.140
188.68.43.28
195.201.179.194
195.201.179.193
198.11.211.210
160.153.206.13
157.7.188.170
186.67.71.106
193.32.161.77
193.32.161.73
83.149.119.178
185.141.25.78
81.17.56.218
172.217.23.52
163.172.236.54
185.163.47.134
172.81.182.63
76.74.177.236
51.77.244.222
107.167.5.93
209.58.147.242
206.189.124.66
89.34.97.112
64.20.38.60
148.66.159.87
122.155.10.189
81.42.220.2
112.165.254.21
95.179.168.23
144.202.19.31
104.129.204.4

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

Contactos

https://www.csirt.gob.cl

+ (562) 24863850

@CSIRTGOB

https://www.linkedin.com/company/csirt-gob

CSIRT
Gobierno de
Chile

Firmado digitalmente por
CSIRT Gobierno de Chile
Fecha: 2019.07.24
18:48:20 -04'00'