13BCS20-00048-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 03 de Abril de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 26 de Marzo y el miércoles 01 de Abril de 2020.

Falsificación de Registro o Identidad

8FFR20-00285-01 CSIRT ADVIERTE DOS SITIOS BANCARIOS FRAUDULENTOS PARA ROBO DE CREDENCIALES

Alerta de seguridad cibernética	8FFR20-00285-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs 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/8ffr20-00285-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00285-01.pdf

8FFR20-00286-01 CSIRT ADVIERTE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00286-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo 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 de 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/8ffr20-00286-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00286-01.pdf

8FFR20-00287-01 CSIRT DETECTÓ PORTAL BANCARIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad cibernética	8FFR20-00287-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco BCI, 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/8ffr20-00287-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00287-01.pdf

8FFR20-00288-01 CSIRT ADVIERTE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00288-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo 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 de 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/8ffr20-00288-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00288-01.pdf

8FFR20-00289-01 CSIRT ADVIERTE ACTIVACIÓN DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00289-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo 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 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/8ffr20-00289-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00289-01.pdf

8FFR20-00290-01 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00290-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco BCI, 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.

Nota: CSIRT reconoce que Andrés Cargill reportó la url a través de redes sociales en paralelo al análisis de nuestra institución. Su nombre no pudo ser incluido en este informe, pero ofrecemos ese reconocimiento y extendemos nuestro agradecimiento por su aporte en este sitio.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00290-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00290-01.pdf

8FFR20-00291-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00291-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial de Banco Falabella, 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/8ffr20-00291-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00291-01.pdf

8FFR20-00292-01 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00292-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Marzo de 2020
Última revisión	28 de Marzo 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 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/8ffr20-00292-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00292-01.pdf

8FFR20-00293-01 CSIRT DETECTA ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00293-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Marzo de 2020
Última revisión	30 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco BCI, 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/8ffr20-00293-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00293-01.pdf

8FFR20-00294-01 CSIRT ADVIERTE LA ACTIVACIÓN DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00294-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte la activación de un portal fraudulento asociado a una IPs 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/8ffr20-00294-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00294-01.pdf

8FFR20-00295-01 CSIRT INFORMA DE LA ACTIVACIÓN DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00295-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo 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 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/8ffr20-00295-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00295-01.pdf

8FFR20-00296-01 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL FRAUDULENTO PARA EL ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad cibernética	8FFR20-00296-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo 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 de Banco BCI, 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/8ffr20-00296-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00296-01.pdf

8FFR20-00297-01 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00297-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril 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 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/8ffr20-00297-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00297-01.pdf

8FFR20-00298-01 CSIRT ADVIERTE ACTIVACIÓN DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00298-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial de Banco Falabella, 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/8ffr20-00298-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00298-01.pdf

8FFR20-00299-01 CSIRT DETECTA ACTIVACIÓN DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00299-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial de Banco BCI, 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/8ffr20-00299-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00299-01.pdf

Malware

2CMV20-00058-01 CSIRT ADVIERTE DE MALWARE POR EMISIÓN DE FACTURA ELECTRÓNICA

Alerta de seguridad cibernética	2CMV20-00058-01
Clase de alerta	Fraude

Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Marzo de 2020
Última revisión	27 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware a través de un correo electrónico que utiliza el nombre de la compañía de Defontana. El mensaje del correo indica que fue generado por la emisión de una factura electrónica. En el cuerpo del correo se dispone de un enlace para la descarga de dicha factura, pero al seleccionar el enlace se produce la descarga de un archivo ZIP, el cual contiene un archivo Html que, al ser ejecutado, direcciona a otro sitio descargando de forma automática otro archivo ZIP, el cual al ser descomprimido, permite obtener otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga del malware.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00058-01/
https://www.csirt.gob.cl/media/2020/03/2CMV20-00058-01.pdf

Phishing

8FPH20-00143-01 CSIRT ADVIERTE PHISHING DE SERVICIO DE STREAMING

Alerta de seguridad cibernética	8FPH20-00143-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparentemente proviene del servicio de streaming Netflix.

El mensaje informa que la cuenta del usuario ha caducado y se suspenderá en 24 horas, por lo que solicita actualizar la información para corregir el problema. El atacante dispone un enlace en el mensaje para ser derivado a un sitio falso que imita a la web oficial del servicio de streaming, en la cual le solicitan ingresar sus credenciales para iniciar una sesión. Luego de eso le solicita al usuario actualizar los datos de la tarjeta de crédito. En estos pasos se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00143-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00143-01.pdf

8FPH20-00144-01 CSIRT ADVIERTE SMISHING EN MENSAJE DE SERVICIO DE STREAMING

Alerta de seguridad cibernética	8FPH20-00144-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de Smishing, que se está difundiendo a través de mensaje de texto falso que aparente proviene de Netflix. El mensaje informa que la suscripción de Netflix se ha suspendido, el atacante dispone un enlace en el mensaje para ser derivado a un sitio falso que imita a la web oficial del servicio de streaming, en la cual le solicita ingresar sus credenciales para iniciar sesión, luego de eso le solicita al usuario actualizar los datos de la tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00144-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00144-01.pdf

8FPH20-00145-01 CSIRT ADVIERTE PHISHING BANCARIO POR REPROGRAMACIÓN DE PAGOS

Alerta de seguridad cibernética	8FPH20-00145-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparenta provenir del Banco Security.

El mensaje informa que el Banco Security como muestra de solidaridad con los clientes, y tomando conciencia del problema de la pandemia COVID-19, opto por reprogramar sus pagos de préstamos, tarjetas de crédito, hipotecarios, créditos vehiculares, créditos por salud y otros servicios que el banco presta. El atacante disponibiliza un enlace para que el cliente autorice las nuevas fechas de pago. Al seleccionar dicho enlace es dirigido a un sitio fraudulento que imita el portal legítimo del banco.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00145-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00145-01.pdf

8FPH20-00146-01 CSIRT ADVIERTE PHISHING BANACARIO POR RETENCIÓN DE TRANSFERENCIA

Alerta de seguridad cibernética	8FPH20-00146-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparenta provenir del Banco Estado.

El mensaje del correo indica, a quien lo recibe, que posee una transferencia retenida, por lo tanto, se debe verificar su identidad en el enlace que se encuentra en el correo. De no realizar esta acción la se advierte a la persona que deberá acercarse a una sucursal para desbloquear la cuenta. Si una persona selecciona el enlace será dirigida a un sitio semejante al del banco, donde se expone al robo de sus credenciales

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00146-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00146-01.pdf

8FPH20-00147-01 CSIRT ADVIERTE PHISHING POR FALSO ANIVERSARIO DE SUPERMERCADO

Alerta de seguridad cibernética	8FPH20-00147-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Marzo de 2020
Última revisión	29 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing vía WhatsApp. El mensaje indica a quienes lo reciben que el supermercado Jumbo está de aniversario y, como promoción especial, está regalando un cupón de $50.000 pesos para celebrar. El atacante disponibiliza un vínculo para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionado a un sitio semejante al del supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades de WhatsApp (20 amigos o 5 grupos), acción necesaria para obtener un cupón. Luego de realizar el paso anterior es direccionado a un sitio semejante al de Jumbo, solicitando las credenciales de acceso. De esta forma el atacante obtiene los datos de la víctima, además de propaga a través de sus contactos de WhatsApp la estafa.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00147-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00147-01.pdf

8FPH20-00148-01 CSIRT ADVIERTE CAMPAÑAS DE PHISHING POR BLOQUEO DE CUENTAS

Alerta de seguridad cibernética	8FPH20-00148-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Marzo de 2020
Última revisión	30 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de correos electrónicos falsos que aparentan provenir del Banco Estado.

Los correos asociados a esta campaña tienen ligeras variaciones en sus asuntos, pero en todos los casos explican al cliente que fue detectada una inconsistencia en los registros del banco respecto a la propia cuenta o de algún servicio asociado, razón por la cual, se procedió al bloqueo de ésta. Para desbloquear la cuenta, el atacante disponibiliza un enlace en el cuerpo del correo, el cual lleva la víctima hasta un sitio similar al del banco donde se expone a la pérdida de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8foh20-00148-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00148-01.pdf

8FPH20-00149-01 CSIRT ADVIERTE CAMPAÑA DE SMISHING BANCARIO POR TRANSFERENCIA

Alerta de seguridad cibernética	8FPH20-00149-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de SMiShing a través de un mensaje de texto que intenta engañar a los usuarios del Banco BCI. El mensaje indica que se realizó una transferencia de 100.500 pesos desde su cuenta a otro banco. El atacante disponibiliza un enlace para que la persona sea dirigido a un sitio web semejante al del banco, para luego robar sus credenciales de acceso y coordenadas del MultipAss.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00149-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00149-01.pdf

8FPH20-00150-01 CSIRT ADVIERTE DE PHISHING CON FALSA PROMOCIÓN DE SUPERMERCADO

Alerta de seguridad cibernética	8FPH20-00150-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing vía WhatsApp, indicando a quienes lo reciben que el supermercado Jumbo se encuentra de aniversario y, como promoción especial, está regalando un cupón de $50.000 pesos para celebrar. El atacante disponibiliza un vínculo para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionado a un sitio semejante al del supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades en WhatsApp (20 amigos o 5 grupos), acción necesaria para obtener su cupón. Luego de realizar el paso anterior es direccionado a un sitio semejante al de Jumbo, solicitando las credenciales de acceso. De esta forma el atacante obtiene sus credenciales y además propaga a través de sus contactos de WhatsApp la estafa.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00150-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00150-01.pdf

8FPH20-00151-01 CSIRT ADVIERTE DE PHISHING POR AVANCE DISPONIBLE EN TARJETA DE CRÉDITO

Alerta de seguridad cibernética	8FPH20-00151-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparente provenir de Cencosud.

El mensaje del correo le indica a la víctima que posee un avance el cual puede simular ingresando al enlace que se encuentra en el cuerpo del correo. Si una persona selecciona el enlace será dirigido a un sitio que simula ser el de la tarjeta Cencosud, donde se expone al robo de sus credenciales asociadas a la tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00151-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00151-01.pdf

9VSA20-00164-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR APPLE PARA IOS, WATCHOS, IPADOS Y SAFARI

Alerta de seguridad cibernética	9VSA20-00164-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Marzo de 2020
Última revisión	30 de Marzo de 2020

Vulnerabilidad

CVE-2020-3883
CVE-2020-3885
CVE-2020-3887
CVE-2020-3888
CVE-2020-3890
CVE-2020-3891
CVE-2020-3894
CVE-2020-3895
CVE-2020-3897
CVE-2020-3899
CVE-2020-3900
CVE-2020-3901
CVE-2020-3902
CVE-2020-3909
CVE-2020-3910
CVE-2020-3913
CVE-2020-3914
CVE-2020-3916
CVE-2020-3919
CVE-2020-9768
CVE-2020-9770
CVE-2020-9773
CVE-2020-9775
CVE-2020-9777
CVE-2020-9780
CVE-2020-9781
CVE-2020-9783
CVE-2020-9784
CVE-2020-9785

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Apple referente a diversas vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00164-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00164-01.pdf

9VSA20-00165-01 CSIRT COMPARTE ACTUALIZACIONES PARA KUBERNETES

Alerta de seguridad cibernética	9VSA20-00165-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo de 2020

Vulnerabilidad

CVE-2020-8551
CVE-2020-8552

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida desde el repositorio oficial de Kubernetes referente a dos vulnerabilidades que afectan al contenedor. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00165-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00165-01.pdf

9VSA20-00166-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR GOOGLE PARA CHROME

Alerta de seguridad cibernética	9VSA20-00166-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Abril de 2020
Última revisión	01 de Abril de 2020

Vulnerabilidad

CVE-2020-6450
CVE-2020-6451
CVE-2020-6452

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a tres vulnerabilidades que afectan al explorador web Google Chrome. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00166-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00166-01.pdf

9VSA20-00162-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PRODUCTOS CISCO

Alerta de seguridad cibernética	9VSA20-00162-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Marzo de 2020
Última revisión	23 de Marzo de 2020

Vulnerabilidad

CVE-2020-3167
CVE-2020-3171
CVE-2020-3172
CVE-2020-3166
CVE-2019-16012
CVE-2019-16010
CVE-2020-3264
CVE-2020-3266
CVE-2020-3265

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Cisco referente a diversas vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00162-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00162-01.pdf

9VSA20-00163-01 CSIRT INFORMA DE VULNERABILIDAD EN WINDOWS ADOBE TYPE MANAGER LIBRARY

Alerta de seguridad cibernética	9VSA20-00163-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Marzo de 2020
Última revisión	23 de Marzo de 2020

Vulnerabilidad

ADV200006

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Microsoft referente a vulnerabilidad crítica aún no parchada (ADV200006) que afecta a la librería Windows Adobe Type Manager Library, para la cual Microsoft recomienda una solución alterna.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00163-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00163-01.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
192.241.238.248	Port Scan
54.180.94.33	Port Scan
64.71.79.132	Port Scan
194.26.29.115	Port Scan
103.91.210.174	DDoS
103.91.211.239	DDoS
45.143.220.236	Port Scan
138.97.220.170	Port Scan
104.194.11.244	Port Scan
198.199.115.203	Port Scan
24.224.174.12	Port Scan
80.82.77.240	Port Scan
45.143.221.53	Port Scan
162.243.129.221	Port Scan
223.74.44.87	DDoS
111.199.185.97	DDoS
27.10.105.161	DDoS
183.211.166.176	DDoS
110.184.59.212	DDoS
27.189.222.255	DDoS
111.61.124.37	DDoS
119.145.128.184	DDoS
221.196.45.211	DDoS
112.51.59.230	DDoS
175.24.95.30	DDoS
43.241.50.40	DDoS
183.136.204.197	DDoS
47.97.90.143	DDoS

120.27.235.43	DDoS
103.45.251.220	DDoS
81.177.143.31	DDoS
189.215.136.49	DDoS
220.134.184.172	DDoS
51.79.57.12	Port Scan
192.241.238.153	Port Scan
213.136.73.44	Port Scan
162.243.132.27	Port Scan
162.243.131.219	Port Scan
195.231.8.23	Port Scan
5.182.210.101	Port Scan
144.91.97.120	Port Scan
192.241.237.102	Port Scan
104.243.43.2	Port Scan
31.14.40.194	Port Scan
163.172.8.228	Port Scan
185.53.88.43	Port Scan
115.28.106.101	DDoS
163.247.93.134	DDoS
60.215.138.14	DDoS
60.215.138.22	DDoS
123.129.192.13	DDoS
123.129.192.21	DDoS
60.215.138.170	DDoS
219.128.128.82	DDoS
60.215.138.168	DDoS
60.215.138.245	DDoS
60.215.138.229	DDoS
60.215.138.166	DDoS
46.105.112.107	Malware
37.139.0.226	Malware
51.75.28.134	Malware
199.195.253.241	Port Scan
108.67.19.208	Port Scan
162.243.130.119	Port Scan
141.98.10.55	Port Scan
106.13.30.203	DDoS
185.62.188.204	Malware
63.142.252.21	Malware
89.46.106.48	Malware

194.0.131.41	Malware
192.241.237.210	Port Scan
103.142.24.39	Malware
176.223.123.55	Malware
217.70.184.38	Malware
195.130.73.229	Malware
66.206.18.186	Malware
198.54.114.254	Malware
162.255.119.103	Malware
157.230.98.85	Malware
192.254.186.250	Malware
81.2.196.60	Malware
162.255.119.86	Malware
164.132.116.247	Malware
173.249.53.59	Malware
51.158.147.3	Malware
37.34.57.30	Malware
188.72.205.231	Malware
104.24.124.250	Malware
70.32.23.20	Malware
54.39.92.49	Malware
23.0.152.140	Malware
92.53.96.240	Malware
192.64.119.119	Malware
162.255.119.61	Malware
45.92.9.74	Malware
192.64.119.93	Malware
5.39.109.102	Malware
193.203.39.244	Malware
198.27.68.204	Malware
194.58.112.174	Malware
2.57.89.31	Malware
91.218.230.159	Malware
185.156.42.49	Malware
162.241.74.163	Malware
88.212.247.4	Malware
103.57.211.14	Malware
96.45.83.55	Malware
199.188.200.93	Malware
192.64.119.126	Malware
93.89.224.101	Malware

80.211.21.116	Malware
217.182.156.218	Malware
95.216.121.171	Malware
89.221.213.66	Malware
185.165.123.36	Malware
192.151.159.178	Malware
92.53.96.189	Malware
213.159.212.174	Malware
176.31.124.7	Malware
81.88.48.71	Malware
92.53.96.189	Malware
95.215.19.12	Malware
31.31.198.157	Malware
148.251.160.39	Malware
162.242.150.89	Malware
185.210.93.19	Malware
192.64.119.145	Malware
79.150.249.94	Malware
141.98.10.37	Port Scan
208.100.26.234	Phishing
37.140.192.153	Malware
206.189.46.218	Malware
192.64.119.28	Malware
162.255.119.113	Malware
162.255.119.153	Malware
143.95.80.46	Malware
65.254.248.151	Malware
51.68.35.162	Malware
185.104.29.28	Malware
181.118.173.144	DDoS
176.119.29.73	Port Scan
85.95.201.3	Port Scan
172.104.229.116	Port Scan
185.175.93.106	Port Scan
184.105.247.216	Port Scan
162.250.98.200	Port Scan
195.231.7.193	Port Scan
62.171.175.20	Port Scan
193.232.142.17	Malware
162.241.61.53	Phishing
45.113.203.193	DDoS

45.113.201.109	DDoS
43.248.187.237	DDoS
212.129.241.64	DDoS
39.101.216.81	DDoS
199.249.230.89	DDoS
89.234.157.254	DDoS
185.220.101.22	DDoS
195.176.3.23	DDoS
142.44.156.149	DDoS
185.220.102.24	DDoS
162.247.74.213	DDoS
109.70.100.31	DDoS
178.165.72.177	DDoS
109.70.100.33	DDoS
162.243.128.20	Port Scan
23.225.172.10	Port Scan
185.175.93.11	Port Scan
92.63.196.22	Port Scan
103.145.13.6	Port Scan
142.44.156.149	DDoS
109.70.100.31	DDoS
109.70.100.33	DDoS
205.185.113.30	DDoS
185.10.68.217	DDoS
199.19.224.76	DDoS
51.15.37.97	DDoS
185.244.39.233	DDoS
193.218.118.130	DDoS
51.75.64.23	DDoS
185.220.101.249	DDoS
109.70.100.24	DDoS
109.248.11.157	DDoS
109.70.100.23	DDoS
209.141.45.189	DDoS
51.75.144.43	DDoS
51.89.200.100	DDoS
45.67.14.0	DDoS
185.220.101.246	DDoS
192.241.237.195	Port Scan
162.243.130.42	Port Scan
162.243.129.184	Port Scan

162.243.128.195	Port Scan
162.243.133.206	Port Scan
192.241.238.4	Port Scan
162.243.130.38	Port Scan
194.26.29.120	Port Scan
195.231.9.234	Port Scan
185.175.93.24	Port Scan
94.102.49.137	Port Scan
185.153.198.240	Port Scan
194.26.29.106	Port Scan
185.175.93.6	Port Scan
162.213.254.115	Port Scan
194.26.29.119	Port Scan
194.26.29.118	Port Scan
208.91.109.90	Port Scan
185.175.93.23	Port Scan
80.211.29.8	Phishing

Url	Motivo
https[:]//www.dieselmoreno.cl/con/cdxxv2_encrypted_81FACBF.bin	Malware
http[:]//www.dieselmoreno.cl/con/cdxxv2_encrypted_81facbf.bin	Malware
http[:]//www.dieselmoreno.cl/con/cdxxv2_encrypted_81FACBF.bin	Malware
http[:]//www.lapurisima.cl/scv.exe	Malware
http[:]//myhood.cl/scan505329.doc	Malware
http[:]//myhood.cl/Scan495082.doc	Malware

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.

- Patricio Jofré. Twitter: https://twitter.com/CasperNear
- Andrés Cargill. Twitter: https://twitter.com/andrescargill
- Gabriel Díaz
- Maurizio Mattoli

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: 2020.04.03 13:11:42 -03'00'