# CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 27 de Marzo de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 19 y el miércoles 25 de Marzo de 2020.

## Falsificación de Registro o Identidad

### 8FFR20-00271-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00271-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Marzo de 2020 |
| Última revisión | 19 de Marzo de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres 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/8ffr20-00271-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00271-01.pdf

## 8FFR20-00272-01 CSIRT ADVIERTE DE 3 PORTALES FRAUDULENTOS QUE SUPLANTAN SITIOS BANCARIOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00272-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Marzo de 2020 |
| Última revisión | 19 de Marzo de 2020 |

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de Banco Estado, el 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/alertas/8ffr20-00272-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00272-01.pdf

## 8FFR20-00273-01 CSIRT INFORMA DE PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00273-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Marzo de 2020 |
| Última revisión | 19 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/8ffr20-00273-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00273-01.pdf

## 8FFR20-00274-01 CSIRT INFORMA DE PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00274-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Marzo de 2020 |
| Última revisión | 19 de Marzo de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), informa de la activación de un portal fraudulento asociado 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.

CSIRT agradece la colaboración de Pablo Cruces Araya para la identificación de este sitio fraudulento, y anima a todas las personas que encuentren vulnerabilidades o incidentes de seguridad cibernética para que los reporten al sitio web https://www.csirt.gob.cl/ o al teléfono + (562) 24863850.

**Enlace:**

https://www.csirt.gob.cl/alertas/8ffr20-00274-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00274-01.pdf

## 8FFR20-00275-01 CSIRT DETECTA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00262-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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 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/8ffr20-00275-01/

https://www.csirt.gob.cl/media/2020/03/8FFR20-00275-01.pdf

## 8FFR20-00276-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00276-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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/8ffr20-00276-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00276-01.pdf

## 8FFR20-00277-01 CSIRT ADVIERTE ACTIVACIÓN DE SITIO WEB BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00277-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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 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/8ffr20-00277-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00277-01.pdf

## 8FFR-00278-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00278-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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 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-00278-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00278-01.pdf

## 8FFR20-00279-01 CSIRT ADVIERTE ACTIVACIÓN DE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00279-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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/8ffr20-00279-01/
https://www.csirt.gob.cl/media/2020/03/8FF20R-00279-01.pdf

## 8FFR20-00280-01 CSIRT ADVIERTE DE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00280-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de Marzo de 2020 |
| Última revisión | 21 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/8ffr20-00280-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00280-01.pdf

## 8FFR20-00281-01 CSIRT ADVIERTE DE 2 PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00281-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Marzo de 2020 |
| Última revisión | 24 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 del 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/8ffr20-00281-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00281-01.pdf

## 8FFR20-00282-01 CSIRT IDENTIFICÓ LA ACTIVACIÓN DE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00282-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Marzo de 2020 |
| Última revisión | 24 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 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/8ffr20-00282-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00282-01.pdf

## 8FFR20-00283-01 CSIRT INFORMA DE 3 PÁGINAS BANCARIAS FRAUDULENTAS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00283-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Marzo de 2020 |
| Última revisión | 24 de Marzo de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres 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/8ffr20-00283-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00283-01.pdf

### 8FFR20-00284-01 CSIRT ADVIERTE TRES PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00284-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| 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 la activación de tres portales fraudulentos asociados 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/8ffr20-00284-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00284-01.pdf

## Malware

### 2CMV20-00053-01 CSIRT ADVIERTE DE PHISHING POR DEUDA A TESORERÍA GENERAL

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00053-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Marzo de 2020 |
| Última revisión | 19 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 Tesorería General de la República (TGR).

El mensaje del correo indica que existen obligaciones producto a una liquidación tributaria que se encuentra impaga. El atacante intenta persuadir a los receptores del correo para que seleccionen el enlace adjunto. Si una persona selecciona el enlace se produce la descarga de un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga el malware.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00053-01/
https://www.csirt.gob.cl/media/2020/03/2CMV20-00053-01.pdf

## 2CMV20-00054-01 CSIRT ADVIERTE CAMPAÑA DE MALWARE EN FALSO CORREO DE TESORERÍA

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00054-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 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 Tesorería General de la República (TGR).

El mensaje del correo solo indica que se adjunta el comprobante solicitado. El estafador adjunta una imagen de la declaración mensual del formulario 29 en el cuerpo del correo y disponibiliza un enlace con el mensaje "Descargar Comprobante". Si un usuario selecciona el enlace inicia la descarga de un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión MSI., el cual, al ser ejecutado, gatilla un script que genera la descarga del malware.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00054-01/

https://www.csirt.gob.cl/media/2020/03/2CMV20-00054-01.pdf

## 2CMV20-00055-01 CSIRT IDENTIFICÓ MALWARE DE UN SUPUESTO PEDIDO EN EL CORREO

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00055-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Marzo de 2020 |
| Última revisión | 24 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 cuyo supuesto remitente sería la compañía de Courier Chilexpress.

El mensaje del correo indica que tienen en sus depósitos un pedido a nombre del receptor del correo. El atacante dispone de un código y un enlace para que la persona pueda obtener más información sobre el envío. Al seleccionar el enlace la persona es dirigida a un sitio donde se descarga un archivo ZIP, el cual contiene un archivo Html que al ser ejecutado direcciona a otro sitio donde se descarga de forma automática otro archivo ZIP. Este, una vez que es descomprimido, permite obtener otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga el malware.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00055-01/

https://www.csirt.gob.cl/media/2020/03/2CMV20-00055-01-1.pdf

## 2CMV20-00056-01 CSIRT ADVIERTE DE MALWARE POR PAGO DE SERVICIOS

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00056-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| 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 malware a través de un correo electrónico indicando el pago de algún tipo de servicio. El mensaje del correo indica que se realizó una transferencia electrónica de fondos en la cuenta de quien recibe el correo. El atacante dispone un enlace en el cuerpo del correo, el que supuestamente permite descargar el comprobante del pago. Si una persona selecciona el enlace es dirigido a un sitio donde se descarga un archivo ZIP, la cual contiene un archivo MSI el cual, al ser ejecutado, gatilla un script que inicia la descarga el malware.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00056-01/
https://www.csirt.gob.cl/media/2020/03/2CMV20-00056-01.pdf

## 2CMV20-00057-01 CSIRT ADVIERTE DE MALWARE QUE SUPLANTA A COMPAÑÍA DE SOFTWARE

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00057-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| 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 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 es dirigido a 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/2cmv20-00057-01/
https://www.csirt.gob.cl/media/2020/03/2CMV20-00057-01.pdf

### 8FPH20-00138-01 CSIRT ADVIERTE DE PHISHING POR CRÉDITO DE CONSUMO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00138-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 de Marzo de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco de Estado. El mensaje del correo indica que el cliente podrá refinanciar sus deudas con un crédito de consumo aprobado. El atacante disponibiliza un enlace que permitiría supuestamente solicitar el abono, pero al seleccionarlo la persona es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00138-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00138-01.pdf

### 8FPH20-00139-01 CSIRT ADVIERTE PHISHING BANCARIO POR COVID-19

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00139-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Marzo de 2020 |
| Última revisión | 23 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 aparente provenir del Banco de Chile.

El mensaje del correo apela a las condiciones de la emergencia producto de la pandemia de Coronavirus y hace un llamado a los clientes de la entidad bancaria a permanecer en sus casas y privilegiar el uso las sucursales virtuales. Aprovechando esa recomendación, informan a quien recibe el correo, que puede utilizar el enlace disponible en el cuerpo del correo para autorizar la postergación de su crédito de consumo, hipotecario o línea de crédito. Si una persona selecciona el enlace será dirigido a un sitio semejante al del banco, donde se expone al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00139-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00139-01.pdf

## 8FPH20-00140-01 CSIRT ADVIERTE DE PHISHING POR INCONVENIENTE EN SERVICIO DE STREAMING

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00140-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Marzo de 2020 |
| Última revisión | 23 de Marzo de 2020 |

**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 que tienen contratado el servicio streaming de Netflix. El correo indica que existe un inconveniente con la cuenta lo que impediría al usuario del servicio acceder a ella hasta que realice algunas actualizaciones. El atacante disponibiliza un enlace que direcciona a un sitio que se asemeja al oficial, donde se le solicita los datos de la tarjeta de crédito con el propósito de robar su credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00140-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00140-01.pdf

## 8FPH20-00141-01 CSIRT ADVIERTE PHISHING POR WHATSAPP DE SERVICIO DE STREAMING POR COVID-19

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00141-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Marzo de 2020 |
| Última revisión | 23 de Marzo de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de la aplicación de mensajería instantánea WhatsApp. El mensaje informa que debido a la pandemia de Coronavirus en todo el mundo, la compañía de servicios de streaming Netflix está dando algunos “pases gratis” para su plataforma durante el periodo de aislamiento. 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 realizan varias preguntas para engañar al usuario. Independiente de cual sea la respuesta, al final de la encuesta el atacante insta a compartir la promoción a sus contactos de WhatsApp. Además en el mismo sitio se inserta un comentario de supuestos personas que han recibido el beneficio, todo lo anterior, para darle credibilidad a la campaña. Esta campaña genera notificaciones de publicidad en los dispositivos.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00141-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00141-01.pdf

# Vulnerabilidades

## 9VSA20-00159-01 CSIRT COMPARTE ACTUALIZACIONES DE VMWARE

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00159-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 18 de Marzo de 2020 |
| Última revisión | 18 de Marzo de 2020 |

**Vulnerabilidad**

CVE-2020-3950
CVE-2020-3951

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de VMware referente a dos vulnerabilidades que afectan a los productos VMware Fusion, VMware Workstation, VMRC y VMware Horizon Client, las cuales de ser explotadas permitirían a un atacante local realizar ataques de denegación de servicios y ejecutar código arbitrario en el sistema. Este informe incluye la respectiva mitigación.

**Enlace**

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00159-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00159-01.pdf

## 9VSA20-00160-01 CSIRT COMPARTE ACTUALIZACIONES PARA GOOGLE CHROME

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00160-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de Marzo de 2020 |
| Última revisión | 20 de Marzo de 2020 |

**Vulnerabilidad**

CVE-2020-6422
CVE-2020-6424
CVE-2020-6425
CVE-2020-6426
CVE-2020-6427
CVE-2020-6428
CVE-2020-6429
CVE-2020-6449
CVE-2019-20503

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Google referente a múltiples vulnerabilidades que afectan a su navegador Google Chrome, las cuales de ser explotadas, permitirían a un atacante remoto comprometer completamente al sistema afectado. Este informe incluye la respectiva mitigación.

**Enlace**

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00160-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00160-01.pdf

### 9VSA20-00161-01 CSIRT COMPARTE ACTUALIZACIONES DE PHP

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00161-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de Marzo de 2020 |
| Última revisión | 21 de Marzo de 2020 |

**Vulnerabilidad**

CVE-2020-7064
CVE-2020-7066
CVE-2020-7065

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de PHP referente a múltiples vulnerabilidades que afectan a sus componentes, las cuales de ser explotadas permitirían a un atacante remoto obtener acceso a información potencialmente sensible, evadir ciertas medidas de seguridad y hasta comprometer completamente al sistema afectado. Este informe incluye la respectiva mitigación.

**Enlace**

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00161-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00161-01.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 |
|---|---|
| 162.243.131.201 | Port Scan |
| 138.97.220.170 | Port Scan |
| 162.243.130.23 | Port Scan |
| 162.243.130.190 | Port Scan |
| 162.243.128.84 | Port Scan |

| | |
|---|---|
| 173.44.48.14 | DDoS |
| 160.153.133.210 | Phishing |
| 80.211.130.144 | Phishing |
| 122.246.96.100 | DDoS |
| 51.178.41.27 | Phishing |
| 162.241.216.131 | Phishing |
| 162.241.217.162 | Phishing |
| 162.243.128.38 | Port Scan |
| 162.243.132.52 | Port Scan |
| 162.243.133.96 | Port Scan |
| 171.236.57.163 | Port Scan |
| 192.241.194.53 | Port Scan |
| 192.241.203.41 | Port Scan |
| 91.212.38.234 | Port Scan |
| 192.241.237.250 | Port Scan |
| 193.32.163.9 | Port Scan |
| 150.107.8.44 | Port Scan |
| 167.86.126.28 | Port Scan |
| 61.219.11.153 | Port Scan |
| 62.171.157.151 | Port Scan |
| 172.106.144.139 | Port Scan |
| 64.79.67.70 | Port Scan |
| 162.243.128.189 | Port Scan |
| 162.243.128.71 | Port Scan |
| 162.243.129.39 | Port Scan |
| 162.243.132.148 | Port Scan |
| 162.243.133.29 | Port Scan |
| 162.243.133.86 | Port Scan |
| 185.43.209.123 | Port Scan |
| 192.241.235.234 | Port Scan |
| 192.241.238.103 | Port Scan |
| 192.241.238.155 | Port Scan |
| 192.241.238.164 | Port Scan |
| 192.241.238.67 | Port Scan |
| 185.53.88.39 | Port Scan |
| 201.132.92.135 | Port Scan |
| 162.243.132.152 | Port Scan |
| 192.241.239.10 | Port Scan |
| 94.23.33.201 | Port Scan |
| 192.241.231.79 | Port Scan |
| 162.243.131.101 | Port Scan |

| | |
|---|---|
| 162.241.226.16 | Phishing |
| 192.241.239.81 | Port Scan |
| 192.241.238.27 | Port Scan |
| 185.143.223.244 | Port Scan |
| 144.91.80.253 | Port Scan |
| 164.132.73.220 | Port Scan |
| 51.75.52.127 | Port Scan |
| 151.139.128.10 | Malware |
| 162.243.130.107 | Port Scan |
| 24.37.12.146 | Port Scan |
| 37.49.226.119 | Port Scan |
| 46.105.90.16 | Port Scan |
| 77.54.234.77 | DDoS |
| 51.159.53.220 | Port Scan |
| 213.59.4.26 | Port Scan |
| 50.7.146.52 | Malware |
| 50.7.146.60 | Malware |
| 107.174.244.107 | Hacking |
| 89.248.168.51 | Port Scan |
| 86.36.20.20 | Port Scan |
| 104.238.220.208 | Port Scan |
| 176.106.44.138 | Port Scan |
| 185.56.80.220 | Port Scan |
| 194.26.29.121 | Port Scan |
| 209.160.107.145 | Port Scan |
| 192.241.235.159 | Port Scan |
| 62.4.14.123 | Port Scan |
| 80.82.77.232 | Port Scan |
| 89.248.169.94 | Port Scan |
| 93.174.93.123 | Port Scan |
| 162.243.128.220 | Port Scan |
| 162.243.130.252. | Port Scan |
| 162.243.131.115 | Port Scan |
| 162.243.132.71 | Port Scan |
| 192.241.237.44 | Port Scan |
| 192.241.239.55 | Port Scan |
| 192.241.239.68 | Port Scan |
| 51.178.128.136 | Port Scan |
| 207.180.213.253 | Port Scan |
| 45.143.220.248 | Port Scan |
| 162.243.128.25 | Port Scan |

| | |
|---|---|
| 162.243.128.84 | Port Scan |
| 162.243.131.67 | Port Scan |
| 173.249.60.88 | Port Scan |
| 192.241.237.35 | Port Scan |
| 195.88.143.245 | Port Scan |
| 200.9.19.151 | Port Scan |
| 206.189.189.204 | Port Scan |
| 212.35.78.237 | Port Scan |
| 162.243.131.67 | Port Scan |
| 37.49.229.183 | Port Scan |
| 198.54.114.48 | Port Scan |
| 148.66.145.153 | Port Scan |
| 192.241.203.163 | Port Scan |
| 94.102.52.57 | Port Scan |
| 109.233.21.41 | Port Scan |
| 77.247.110.63 | Port Scan |
| 45.79.163.211 | Port Scan |
| 45.143.220.251 | Port Scan |
| 119.28.239.205 | Port Scan |
| 192.241.239.195 | Port Scan |
| 156.96.118.252 | Port Scan |
| 45.9.148.54 | Port Scan |
| 89.248.174.213 | Port Scan |
| 122.53.122.163 | Port Scan |
| 186.105.108.161 | DDoS |
| 115.217.182.142 | Port Scan |
| 195.231.0.174 | Port Scan |
| 185.200.118.73 | Port Scan |
| 185.200.118.73 | Port Scan |
| 162.243.128.215 | Port Scan |
| 62.171.163.89 | Port Scan |
| 80.82.77.248 | Port Scan |
| 162.243.133.180 | Port Scan |
| 15.236.60.157 | Port Scan |
| 100.42.228.66 | Port Scan |
| 113.30.248.56 | Port Scan |
| 162.243.131.132 | Port Scan |
| 162.243.132.170 | Port Scan |
| 162.243.132.87 | Port Scan |
| 173.0.58.202 | Port Scan |
| 185.153.197.10 | Port Scan |

| | |
|---|---|
| 185.153.199.211 | Port Scan |
| 192.241.203.163 | Port Scan |
| 192.241.237.52 | Port Scan |
| 45.143.220.43 | Port Scan |
| 45.143.220.48 | Port Scan |
| 180.214.236.52 | Port Scan |
| 192.241.238.222 | Port Scan |
| 58.82.242.32 | Port Scan |
| 103.145.12.25 | Port Scan |
| 210.18.158.234 | Port Scan |
| 162.243.131.167 | Port Scan |
| 185.36.81.33 | Port Scan |
| 104.26.6.133 | Port Scan |
| 162.243.128.92 | Port Scan |
| 162.243.133.35 | Port Scan |
| 103.253.42.44 | Port Scan |
| 162.243.130.23 | Port Scan |
| 162.243.128.39 | Port Scan |
| 136.144.49.141 | Port Scan |
| 154.16.246.84 | Port Scan |
| 162.243.129.105 | Port Scan |
| 162.243.132.54 | Port Scan |
| 192.241.202.15 | Port Scan |
| 192.241.238.222 | Port Scan |
| 62.171.167.199 | Port Scan |
| 62.210.129.208 | Port Scan |
| 116.86.221.69 | Port Scan |
| 58.182.16.97 | Port Scan |
| 77.247.109.73 | Port Scan |
| 46.101.94.224 | Port Scan |
| 45.232.32.130 | Port Scan |
| 192.241.238.171 | Port Scan |
| 80.211.252.81 | Port Scan |
| 66.42.98.220 | Hacking |
| 212.129.63.209 | Port Scan |
| 109.238.11.190 | Port Scan |
| 207.180.196.144 | Port Scan |
| 213.59.4.26 | DDoS |
| 1.198.7.61 | DDoS |
| 122.228.19.81 | DDoS |
| 185.175.93.100 | DDoS |

| | |
|---|---|
| 185.175.93.105 | DDoS |
| 185.176.27.162 | DDoS |
| 185.176.27.30 | DDoS |
| 223.71.167.165 | DDoS |
| 51.91.212.80 | DDoS |
| 79.124.62.86 | DDoS |

## 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.

- Kevin Sánchez
- Jaime de los Hoyos. Linkedin: https://www.linkedin.com/in/jdeloshoyos/
- Óscar Orellana. Linkedin: http://linkedin.com/in/oscarorellanaa

## 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: 2020.03.26 18:04:33 -03'00'