13BCS20-00052-01

# CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Jueves 30 de Abril de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 23 de Abril y el miércoles 29 de Abril de 2020.

## Falsificación de Registro o Identidad

### 8FFR20-00357-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00357-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Abril de 2020 |
| Última revisión | 23 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres 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/8ffr20-00357-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00357-01.pdf

## 8FFR20-00358-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00358-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Abril de 2020 |
| Última revisión | 23 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 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/8ffr20-00358-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00358-01.pdf

## 8FFR20-00359-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00359-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Abril de 2020 |
| Última revisión | 23 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 suplantan el sitio web oficial de Banco Security, 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/8ffr20-00359-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00359-01.pdf

## 8FFR20-00360-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00360-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 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 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/8ffr20-00360-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00360-01.pdf

## 8FFR20-00361-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00361-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 de Abril 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/8ffr20-00361-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00361-01.pdf

## 8FFR20-00362-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00362-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril 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/8ffr20-00362-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00362-01.pdf

## 8FFR20-00363-01 CSIRT ADVIERTE DE 3 SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00363-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de tres portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco Security, 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/8ffr20-00363-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00363-01.pdf

## 8FFR20-00364-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00364-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril 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/8ffr20-00364-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00364-01.pdf

## 8FFR20-00365-01 CSIRT ADVIERTE DE UN SITIO WEB BANCARIO FRAUDULENTO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00365-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril 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 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/8ffr20-00365-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00365-01.pdf

## 8FFR20-00366-01 CSIRT ADVIERTE DE 5 SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00366-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de cinco 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/8ffr20-00166-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00366-01.pdf

## 8FFR20-00367-01 CSIRT ADVIERTE 4 SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00367-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de cinco portales fraudulentos asociados a dos IP 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/8ffr20-00367-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00367-01.pdf

## 8FFR20-00368-01 CSIRT ADVIERTE DE 5 SITIOS BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00368-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado la activación de cinco portales fraudulentos asociados a dos 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/8ffr20-00368-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00368-01.pdf

## 8FFR20-00369-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00369-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado 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/8ffr20-00369-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00369-01.pdf

## 8FFR20-00370-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00370-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Abril de 2020 |
| Última revisión | 28 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 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/8ffr20-00370-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00370-01.pdf

## 8FFR20-00371-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00371-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 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 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/8ffr20-00371-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00371-01.pdf

## 2CMV20-00059-01 CSIRT ADVIERTE INMINENTE CAMPAÑA DE MALWARE POR COVID-19

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00059-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing-Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Abril de 2020 |
| Última revisión | 23 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), pronostica la activación de varias campañas de phishing con malware asociado utilizando el nombre del virus COVID-19 sobre el ecosistema cibernético chileno en los próximos días. Esta alerta se genera a partir del análisis de múltiples campañas de phishing que utilizan el descargador de malware GuLoader. Éste se caracteriza por sus cargas útiles de malware que se encuentran ubicadas en recursos compartidos en la nube, por ejemplo, en driver.google.com. El atacante intenta persuadir al receptor del correo electrónico que descargue un archivo adjunto que, en la mayoría de los casos, está en formato comprimido Zip, Rar, 7z e ISO, los que contienen archivos ejecutables con el malware GuLoader. La función de estos descargadores de malware es comunicarse en forma cifrada con recursos compartidos de driver.google.com. De esa forma libera las cargas útiles de malware al equipo del usuario, los que de acuerdo las evidencias analizadas, son troyanos de acceso remoto (RAT) diseñados para tomar el control del equipo por el atacante. Estos troyanos se ejecutan sin el consentimiento del usuario, ocultándose en algún proceso legítimo de Windows para no ser detectado por el antivirus o cualquier sistema de detección de amenaza. A partir del análisis de los hash obtenidos en las muestras, se pudo constatar que en los últimos días el malware se ha propagado desde Europa a Latinoamérica, encontrándose rastros de su presencia en Brasil, Argentina, Paraguay, Bolivia, Ecuador y Venezuela, lo que permite concluir que su aparición en Chile sería inminente en cuestión de horas o días. CSIRT comparte en este documento algunos indicadores de compromisos en relación al descargador GuLoader.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00059-01/
https://www.csirt.gob.cl/media/2020/04/2CMV20-00059-01.pdf

### 2CMV20-00060-01 CSIRT INFORMA DE MALWARE DE POR PAGO DE CONTRIBUCIONES

| | |
|---|---|
| Alerta de seguridad cibernética | 2CMV20-00060-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Abril de 2020 |
| Última revisión | 23 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), informa de una campaña de malware a través de un correo electrónico que utiliza el nombre de la Tesorería General de la Republica. El atacante busca que las personas descarguen un archivo malicioso en sus dispositivos.

El mensaje, cuya gramática es deficiente, indica que debido a la información dada en el noticiero del canal público –no especifica un canal de TV-, a partir del 27 de marzo 2020 se habría iniciado la liberación de pago, por concepto de contribuciones, a los pensionados. Posteriormente se menciona que aquellas personas que pagaron a tiempo serían premiadas con un descuento de 70% durante 3 meses. En el cuerpo del correo se dispone de un enlace para verificar si la persona es beneficiaria de este descuento. Al seleccionar el enlace se produce la descarga de un archivo ZIP, el cual, al ser descomprimido, permite obtener otro archivo con extensión MSI. Cuando se ejecuta, se gatilla un script que inicia la descarga del malware.

**Enlace:**

https://www.csirt.gob.cl/alertas/2cmv20-00060-01/

https://www.csirt.gob.cl/media/2020/04/2CMV20-00060-01.pdf

## Phishing

### 8FPH20-00194-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR BLOQUEO DE CUENTA

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00194-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 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 supuestamente proviene del Banco Scotiabank.

Los atacantes buscan persuadir a sus víctimas para utilizar un enlace adjunto en el correo y entregar información personal y bancaria.

El mensaje del correo informa que se detectó un error de afiliación en la banca en línea. El texto utilizado es un tanto confuso al plantear cual sería el error. El mensaje continúa señalando que por

seguridad se procedió al bloqueo de la cuenta de manera temporal hasta que no termine su registro correcto. Los motivos del bloqueo podrían ser el registro de datos personales, el acceso a su cuenta a través de diferentes lugares, o falta activar de la clave 3.0 y superclave.
El atacante disponibiliza un enlace para realizar la supuesta activación. Si una persona selecciona el enlace, será dirigida a un sitio web semejante al del banco, donde se expondrá al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00194-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00194-01.pdf

### 8FPH20-00195-01 CSIRT ADVIERTE DE PHIHSING POR INSUFICIENTE ESPACIO EN CORREO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00195-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 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 que supuestamente proviene de Gmail. El atacante intenta persuadir a las personas para utilizar un enlace en el cuerpo del correo. El mensaje del correo informa a quien lo recibe que el correo no tiene suficiente espacio y como consecuencia, hay algunos correos que permanecen en el servidor pendientes de ser entregados, lo que se pude solucionar si la persona sigue las instrucciones indicadas y utiliza un enlace disponible para liberar espacio automáticamente y hacer posible la entrega de los correos pendientes. De selecciona el enlace la víctima es dirigida a un sitio web con un formulario que indica ser de “gmail.cl” –información relevante considerando que el correo está en inglés-, donde se expondrá al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00195-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00195-01.pdf

## 8FPH20-00196-01 CSIRT ADVIERTE DE PHISHING OFRECIENDO AVANCE EN CUENTA CORRIENTE

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00196-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 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 supuestamente proveniente de Cencosud. El atacante busca que las personas utilicen un enlace que se dispone en el correo. El mensaje informa sobre la opción de solicitar un avance rápido y directo a la cuenta corriente, pagando hasta en 48 cuotas, de forma inmediata y sin trámites. El atacante disponibiliza un enlace para realizar la simulación de crédito. Si la víctima selecciona el enlace será dirigida a un sitio web semejante a Cencosud, donde se expondrá al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00196-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00196-01.pdf

## 8FPH20-00197-01 CSIRT ADVIERTE DE PHISHING POR TRANSFERENCIA DE FONDOS RETENIDA

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00197-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 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 supuestamente proveniente del Banco Scotiabank. El atacante busca que la víctima ingrese a un enlace adjunto en el cuerpo del correo. El mensaje informa que se realizó una transferencia de fondos desde su cuenta y que ésta se encuentra retenida. El atacante disponibiliza un enlace para verificar el estado de cuenta. Al seleccionar el enlace, la víctima es dirigida a un sitio web semejante al del banco, donde se expondrá al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00197-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00197-01.pdf

## 8FPH20-00197-01 CSIRT ADVIERTE DE PHISHING POR TRANSFERENCIA DE FONDOS RETENIDA

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00197-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 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 supuestamente proveniente del Banco Scotiabank. El atacante busca que la víctima ingrese a un enlace adjunto en el cuerpo del correo. El mensaje informa que se realizó una transferencia de fondos desde su cuenta y que ésta se encuentra retenida. El atacante disponibiliza un enlace para verificar el estado de cuenta. Al seleccionar el enlace, la víctima es dirigida a un sitio web semejante al del banco, donde se expondrá al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00197-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00197-01.pdf

## 8FPH20-00198-01 CSIRT ADVIERTE DE PHISHING DE SUPUESTA CUENTA BANCARIA SUSPENDIDA

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00198-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 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 supuestamente proveniente del Banco Estado. El atacante intenta persuadir a las personas para utilizar un enlace en el cuerpo del correo. El mensaje del correo informa que existe un error en los sistemas, que se define como cuenta suspendida, ya que la persona no habría realizado el proceso de verificación de identidad en su cuenta. En mensaje indica que ese procedimiento sería necesario, de lo contrario, el servicio online podría quedar bloqueado para el cliente. El atacante disponibiliza un enlace en el correo para realizar la supuesta verificación. Si una persona selecciona el enlace, será dirigida a un sitio falso del banco donde se expone al robo de sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00198-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00198-01.pdf

## 8FPH20-00189-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR BLOQUEO DE CUENTA

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00189-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 de Abril de 2020 |

**Resumen**

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing supuestamente proveniente del servicio de correo Zimbra. El atacante intenta persuadir a las personas para que utilicen el mensaje adjunto en el cuerpo del correo. El mensaje informa que la contraseña de la persona expirará dentro de 2 días, por lo tanto, para mantener la cuenta activa es necesario seguir unas instrucciones que se explicarán ingresando al enlace. Si una persona selecciona el enlace, será dirigida a un sitio falso del correo corporativo de Zimbra donde se le solicitará el nombre de usuario y contraseña, y podría perder sus credenciales.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00199-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00199-01.pdf

## 8FPH20-00200-01 CSIRT ADVIERTE DE PHISHING POR SERVICIO DE STREAMING SUSPENDIDO

| | |
|---|---|
| Alerta de seguridad cibernética | 8FPH20-00200-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril 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 usurpa al servicio de streaming Netflix. El atacante busca persuadir a quienes reciben el correo para que ingresen a un enlace adjunto en el cuerpo del correo. El mensaje informa que la cuenta del usuario se encuentra suspendida, ya que no se pudo autorizar su pago para el próximo ciclo de facturación, aunque se le garantiza a la persona que la membresía aún está activa. El atacante dispone de un enlace para reiniciar la membresía. Si la persona utiliza el enlace será derivada a un sitio falso que imita a la web oficial del servicio de streaming, en la cual le solicitarán ingresar sus credenciales para iniciar una sesión.

**Enlace:**

https://www.csirt.gob.cl/alertas/8fph20-00200-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00200-01.pdf

## 9VSA20-00187-01 CSIRT COMPARTE ACTUALIZACIONES DE PRESTASHOP PARA SU GESTOR DE CONTENIDOS

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00187-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-5264
CVE-2020-5265
CVE-2020-5269
CVE-2020-5270
CVE-2020-5271
CVE-2020-5272
CVE-2020-5276
CVE-2020-5278
CVE-2020-5279
CVE-2020-5285
CVE-2020-5286
CVE-2020-5287
CVE-2020-5288
CVE-2020-5293

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por PrestaShop referente a vulnerabilidades que afectan al gestor de contenidos. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00187-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00187-01.pdf

## 9VSA20-00188-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR F5 PARA NGINX CONTROLLER

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00188-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de Abril de 2020 |
| Última revisión | 24 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-5863
CVE-2020-5864
CVE-2020-5865
CVE-2020-5866
CVE-2020-5867

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por F5 referente a múltiples vulnerabilidades que afectan a NGINX Controller. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00188-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00188-01.pdf

## 9VSA20-00189-01 CSIRT COMPARTE ACTUALIZACIONES DE SOPHOS PARA SOPHOS XG FIREWALL/SFOS

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00189-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 de Abril de 2020 |
| Última revisión | 27 de Abril de 2020 |

### Vulnerabilidad

CWE-89

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Sophos referente a vulnerabilidad que afecta a Sophos XG Firewall/SFOS. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00189-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00189-01.pdf

## 9VSA20-00190-01 CSIRT COMPARTE ACTUALIZACIÓN LIBERADAS POR ADOBE PARA ADOBE ILLUSTRATOR

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00190-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-9570
CVE-2020-9571
CVE-2020-9572
CVE-2020-9573
CVE-2020-9574

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Adobe referente a múltiples vulnerabilidades que afectan a Adobe Illustrator. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00190-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00190-01.pdf

## 9VSA20-00191-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR FORTINET PARA FORTIMAIL Y FORTIVOICE ENTERPRISE

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00191-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-9294

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por FortiNet referente a vulnerabilidad que afecta a FortiMail y FortiVoice Enterprise. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00191-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00191-01.pdf

## 9VSA20-00192-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR GOOGLE PARA GOOGLE CHROME

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00192-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-6461
CVE-2020-6462

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a vulnerabilidades que afectan a Google Chrome. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00192-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00192-01.pdf

## 9VSA20-00193-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR GRAFANA

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00193-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-12245

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Grafana referente a vulnerabilidad que afecta a su software de visualización de datos. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00193-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00193-01.pdf

## 9VSA20-00194-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR VMWARE PARA VMWAREESXI

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00194-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-3955

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMware referente a vulnerabilidad que afecta a VMware ESXi. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00194-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00194-01.pdf

## 9VSA20-00195-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR SAMBA

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA20-00195-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 de Abril de 2020 |
| Última revisión | 29 de Abril de 2020 |

### Vulnerabilidad

CVE-2020-10700
CVE-2020-10704

### Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Samba referente a vulnerabilidad que afecta al protocolo de archivos compartidos. El presente informe incluye la respectiva medida de mitigación.

### Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00195-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00195-01.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 |
|---|---|
| 8.209.76.143 | Malware |
| 160.153.129.213 | Malware |
| 8.209.76.143 | Malware |
| 8.209.76.143 | Malware |
| 162.159.134.233 | Malware |
| 208.113.152.109 | Phishing |
| 45.77.229.248 | SQLi Attempt |
| 162.243.128.105 | Port Scan |
| 162.243.130.197 | Port Scan |
| 50.116.17.183 | Port Scan |
| 103.231.161.78 | Port Scan |
| 103.231.161.77 | Port Scan |
| 103.231.161.72 | Port Scan |
| 103.231.161.73 | Port Scan |
| 103.231.161.75 | Port Scan |
| 103.231.161.79 | Port Scan |
| 103.231.161.76 | Port Scan |
| 103.231.161.74 | Port Scan |
| 162.243.131.210 | Port Scan |
| 123.253.88.55 | Port Scan |
| 68.183.170.114 | Port Scan |
| 198.199.119.98 | Port Scan |
| 162.243.131.167 | Port Scan |
| 103.133.109.107 | Port Scan |
| 185.168.227.238 | Port Scan |
| 162.243.128.251 | Port Scan |
| 1.162.144.24 | Port Scan |
| 189.50.252.238 | Port Scan |
| 220.92.153.250 | Port Scan |
| 220.142.162.25 | Port Scan |
| 162.243.130.163 | Port Scan |
| 162.243.128.177 | Port Scan |
| 185.150.190.103 | Port Scan |

| | |
|---|---|
| 192.241.224.172 | Port Scan |
| 162.243.130.125 | Port Scan |
| 162.243.128.167 | Port Scan |
| 162.243.130.183 | Port Scan |
| 103.122.14.40 | Port Scan |
| 192.241.237.6 | Port Scan |
| 192.241.231.98 | Port Scan |
| 162.243.130.175 | Port Scan |
| 84.13.204.238 | Port Scan |
| 162.243.129.58 | Port Scan |
| 162.243.128.69 | Port Scan |
| 122.155.6.206 | Port Scan |
| 185.123.101.128 | Port Scan |
| 45.79.28.132 | Port Scan |
| 117.4.115.55 | Port Scan |
| 14.170.220.203 | Port Scan |
| 85.103.62.106 | Port Scan |
| 27.73.88.226 | Port Scan |
| 113.160.82.166 | Port Scan |
| 171.236.48.115 | Port Scan |
| 113.212.112.4 | Port Scan |
| 184.82.25.206 | Port Scan |
| 49.145.205.78 | Port Scan |
| 14.188.169.249 | Port Scan |
| 101.108.122.118 | Port Scan |
| 58.186.14.22 | Port Scan |
| 116.97.214.42 | Port Scan |
| 118.173.204.221 | Port Scan |
| 14.181.33.62 | Port Scan |
| 14.176.200.233 | Port Scan |
| 37.194.225.63 | Port Scan |
| 49.68.246.198 | Port Scan |
| 78.108.184.198 | Malware |
| 162.243.128.36 | Port Scan |
| 192.241.232.227 | Port Scan |
| 192.241.234.109 | Port Scan |
| 162.243.130.26 | Port Scan |
| 162.243.131.9 | Port Scan |
| 162.243.130.121 | Port Scan |
| 195.154.28.229 | Port Scan |
| 79.122.53.88 | Port Scan |

| | |
|---|---|
| 223.146.37.224 | Port Scan |
| 1.162.144.25 | Port Scan |
| 1.162.144.56 | Port Scan |
| 1.168.117.60 | Port Scan |
| 36.226.177.68 | Port Scan |
| 36.228.26.89 | Port Scan |
| 113.22.166.86 | Port Scan |
| 1.172.55.129 | Port Scan |
| 118.71.213.249 | Port Scan |
| 2.132.212.236 | Port Scan |
| 36.229.252.38 | Port Scan |
| 220.141.52.11 | Port Scan |
| 118.68.33.131 | Port Scan |
| 112.72.79.3 | Port Scan |
| 42.118.148.73 | Port Scan |
| 113.22.170.10 | Port Scan |
| 47.254.213.81 | Port Scan |
| 183.80.22.226 | Port Scan |
| 180.93.14.162 | Port Scan |
| 77.247.110.88 | Port Scan |
| 162.243.129.215 | Port Scan |
| 192.241.236.248 | Port Scan |
| 162.243.129.180 | Port Scan |
| 192.241.239.251 | Port Scan |
| 162.243.130.40 | Port Scan |
| 162.243.128.43 | Port Scan |
| 210.137.6.37 | Port Scan |
| 217.117.4.110 | Port Scan |
| 192.241.238.64 | Port Scan |
| 218.255.24.226 | Port Scan |
| 162.243.131.78 | Port Scan |
| 221.138.17.152 | Port Scan |
| 26.165.218.44 | Port Scan |
| 47.206.4.145 | Port Scan |
| 70.224.36.194 | Port Scan |
| 81.94.192.10 | Port Scan |
| 81.94.192.147 | Port Scan |
| 84.49.242.125 | Port Scan |
| 97.90.44.200 | Port Scan |
| 14.207.152.122 | Port Scan |
| 80.211.91.172 | Port Scan |

| | |
|---|---|
| 80.82.78.100 | Port Scan |
| 45.148.10.179 | Port Scan |
| 54.37.200.119 | Port Scan |
| 185.222.58.133 | Port Scan |
| 194.34.134.207 | Port Scan |
| 1.172.55.129 | Port Scan |
| 162.243.130.86 | Port Scan |
| 162.243.131.186 | Port Scan |
| 162.243.131.22 | Port Scan |
| 192.241.237.175 | Port Scan |
| 192.241.231.118 | SSH Attempt |
| 125.160.17.32 | SSH Attempt |
| 139.162.122.110 | SSH Attempt |
| 182.253.70.89 | SSH Attempt |
| 195.88.142.204 | SSH Attempt |
| 101.109.115.27 | SSH Attempt |
| 122.54.175.202 | SSH Attempt |
| 137.74.53.155 | SSH Attempt |
| 209.141.35.177 | SSH Attempt |
| 14.171.191.243 | SSH Attempt |
| 36.89.135.79 | SSH Attempt |
| 157.245.104.96 | SSH Attempt |
| 45.55.23.144 | SSH Attempt |
| 164.52.24.164 | SSH Attempt |
| 189.195.41.134 | SSH Attempt |
| 197.231.70.60 | SSH Attempt |
| 219.93.106.33 | SSH Attempt |
| 45.148.10.91 | SSH Attempt |
| 51.38.36.84 | SSH Attempt |
| 5.13.34.133 | SSH Attempt |
| 60.251.229.67 | SSH Attempt |
| 75.127.13.67 | SSH Attempt |
| 65.49.20.66 | SSH Attempt |
| 79.27.235.172 | SSH Attempt |
| 81.136.255.20 | SSH Attempt |
| 92.118.27.202 | SSH Attempt |
| 82.64.140.9 | SSH Attempt |
| 95.156.31.74 | SSH Attempt |
| 115.112.61.220 | SSH Attempt |
| 84.92.39.93 | SSH Attempt |
| 103.56.207.117 | SSH Attempt |

| | |
|---|---|
| 31.165.11.9 | SSH Attempt |
| 103.72.8.7 | SSH Attempt |
| 165.22.93.239 | IP_Src_session |
| 192.241.220.35 | UDP_Src_session |
| 162.243.135.103 | Port Scan |
| 192.241.224.81 | Port Scan |
| 192.241.235.86 | Port Scan |
| 192.241.223.106 | Port Scan |
| 185.53.88.126 | Port Scan |
| 162.243.135.115 | Port Scan |
| 162.243.130.198 | Port Scan |
| 192.241.224.81 | Port Scan |
| 192.241.220.215 | Port Scan |
| 162.243.133.91 | Port Scan |
| 70.36.103.235 | Port Scan |
| 140.238.225.206 | Port Scan |
| 178.173.203.159 | Port Scan |
| 92.118.234.202 | Port Scan |
| 172.81.129.216 | Port Scan |
| 5.145.86.46 | Port Scan |
| 79.112.194.149 | Port Scan |
| 86.123.36.217 | Port Scan |
| 162.243.132.6 | Port Scan |
| 162.243.134.201 | Port Scan |
| 192.241.203.139 | Port Scan |
| 192.241.208.65 | Port Scan |
| 192.241.219.25 | Port Scan |
| 192.241.222.28 | Port Scan |
| 198.199.105.231 | Port Scan |
| 210.186.147.107 | Port Scan |
| 218.212.42.143 | Port Scan |
| 86.98.86.126 | Port Scan |
| 162.243.132.159 | Port Scan |
| 192.241.232.88 | Port Scan |
| 14.254.87.160 | Port Scan |
| 192.241.238.183 | Port Scan |
| 23.237.55.10 | Port Scan |
| 162.243.129.51 | Port Scan |
| 162.243.132.7 | Port Scan |
| 162.243.132.157 | Port Scan |
| 27.77.77.148 | Port Scan |

| | |
|---|---|
| 162.243.132.165 | Port Scan |
| 162.243.134.225 | Port Scan |
| 192.241.213.129 | Port Scan |
| 45.143.221.47 | Port Scan |
| 192.241.219.143 | Port Scan |
| 156.218.229.248 | Port Scan |
| 193.31.40.36 | Port Scan |
| 192.241.198.105 | Port Scan |
| 193.31.40.37 | Port Scan |
| 45.143.220.200 | Port Scan |
| 192.241.223.231 | Port Scan |
| 192.241.238.152 | Port Scan |
| 77.247.110.39 | Port Scan |
| 192.241.237.102 | Port Scan |
| 192.241.210.125 | Port Scan |
| 162.243.134.64 | Port Scan |
| 192.241.211.113 | Port Scan |
| 192.241.238.229 | Port Scan |
| 192.241.237.187 | Port Scan |
| 162.243.135.71 | Port Scan |
| 198.199.105.154 | Port Scan |
| 192.241.224.19 | Port Scan |
| 192.241.208.144 | Port Scan |
| 192.241.227.177 | Port Scan |
| 192.241.233.208 | Port Scan |
| 162.243.130.234 | Port Scan |
| 192.241.231.174 | Port Scan |
| 192.241.133.191 | Malware |
| 43.255.30.111 | Malware |
| 103.108.195.89 | Malware |
| 143.92.56.10 | Malware |
| 186.10.66.139 | Malware |
| 192.241.223.140 | Port Scan |
| 192.241.227.88 | Port Scan |
| 125.104.198.245 | Port Scan |
| 125.104.205.200 | Port Scan |
| 115.214.203.114 | Port Scan |
| 183.152.216.128 | Port Scan |
| 125.122.215.57 | Port Scan |
| 162.243.136.76 | Port Scan |
| 162.243.136.41 | Port Scan |

| | |
|---|---|
| 51.159.30.47 | Port Scan |
| 62.171.142.207 | Port Scan |
| 162.243.135.221 | Port Scan |
| 162.243.135.9 | Port Scan |
| 36.91.107.125 | Port Scan |
| 162.243.134.169 | Port Scan |
| 103.88.129.71 | Port Scan |
| 172.104.241.110 | Port Scan |
| 221.140.57.201 | Port Scan |
| 192.241.213.146 | Port Scan |
| 198.199.117.93 | Port Scan |
| 192.64.112.32 | Port Scan |
| 31.14.40.94 | Port Scan |
| 162.243.133.176 | Port Scan |
| 114.34.72.141 | Port Scan |
| 162.243.134.111 | Port Scan |
| 111.241.199.110 | Port Scan |
| 118.163.41.12 | Port Scan |
| 88.232.5.11 | Port Scan |
| 174.138.183.59 | Port Scan |
| 188.217.238.230 | Port Scan |
| 36.232.69.137 | Port Scan |
| 114.40.188.138 | Port Scan |
| 78.47.123.172 | Malware |
| 78.47.121.243 | Malware |
| 199.231.85.124 | Malware |
| 78.47.121.241 | Malware |
| 45.9.148.125 | Malware |
| 5.9.163.18 | Malware |
| 107.191.99.95 | Malware |
| 107.191.99.221 | Malware |
| 45.9.148.129 | Malware |
| 45.9.148.117 | Malware |
| 94.130.193.148 | Malware |
| 94.130.193.147 | Malware |
| 94.130.193.146 | Malware |
| 94.130.165.87 | Malware |
| 5.9.163.19 | Malware |
| 212.83.146.233 | Malware |
| 68.183.89.155 | Phishing |
| 134.209.145.156 | Phishing |

| | |
|---|---|
| 45.152.6.58 | Port Scan |
| 94.1.138.47 | Port Scan |
| 105.157.228.40 | Port Scan |
| 162.243.133.57 | Port Scan |
| 162.243.133.95 | Port Scan |
| 162.243.134.131 | Port Scan |
| 162.243.135.167 | Port Scan |
| 187.93.145.58 | Port Scan |
| 192.241.211.106 | Port Scan |
| 192.241.234.246 | Port Scan |
| 199.59.242.153 | Phishing |
| 159.203.95.247 | Phishing |
| 36.170.14.2 | DdoS |
| 49.212.131.155 | Port Scan |
| 203.143.72.235 | Phishing |
| 198.199.113.198 | Port Scan |
| 186.67.71.53 | Phishing |
| 192.241.238.205 | Port Scan |
| 192.241.212.205 | Port Scan |
| 192.241.210.186 | Port Scan |
| 192.241.239.192 | Port Scan |
| 168.235.111.4 | Port Scan |
| 139.162.31.12 | Port Scan |
| 162.243.134.90 | Port Scan |
| 162.243.135.126 | Port Scan |
| 188.227.84.88 | Port Scan |
| 192.241.208.234 | Port Scan |
| 192.241.237.8 | Port Scan |
| 162.243.131.223 | Port Scan |
| 162.243.132.128 | Port Scan |
| 162.243.136.131 | Port Scan |
| 192.241.226.10 | Port Scan |
| 192.241.235.57 | Port Scan |
| 192.241.237.209 | Port Scan |
| 185.164.72.112 | DdoS |
| 192.241.238.11 | Port Scan |
| 192.241.238.154 | Port Scan |
| 192.241.238.210 | Port Scan |
| 192.241.238.245 | Port Scan |
| 192.241.239.123 | Port Scan |
| 162.243.134.66 | Port Scan |

| | |
|---|---|
| 162.243.136.51 | Port Scan |
| 162.243.133.116 | Port Scan |
| 192.241.225.221 | Port Scan |
| 192.241.209.7 | Port Scan |
| 192.241.235.87 | Port Scan |
| 162.243.134.66 | Port Scan |
| 193.142.146.53 | Port Scan |
| 192.241.227.213 | Port Scan |
| 192.241.225.162 | Port Scan |
| 162.243.133.233 | Port Scan |
| 192.241.221.16 | Port Scan |
| 111.121.77.153 | DdoS |
| 120.230.164.64 | DdoS |
| 124.89.78.169 | DdoS |
| 222.212.13.68 | DdoS |
| 59.42.39.51 | DdoS |
| 202.96.102.244 | DdoS |
| 27.153.71.211 | DdoS |
| 111.163.118.2 | DdoS |
| 125.73.104.191 | DdoS |
| 60.180.195.206 | DdoS |
| 206.189.74.166 | Port Scan |
| 92.249.44.4 | Phishing |
| 165.22.223.114 | Phishing |
| 51.253.85.168 | Port Scan |
| 74.63.223.110 | Port Scan |
| 162.243.131.97 | Port Scan |
| 162.243.131.200 | Port Scan |
| 192.241.239.179 | Port Scan |
| 192.241.220.151 | Port Scan |
| 192.241.212.239 | Port Scan |
| 185.244.39.76 | Port Scan |
| 162.243.136.15 | Port Scan |
| 45.56.77.175 | Malware |
| 185.103.156.5 | Malware |
| 46.182.5.20 | Malware |
| 195.22.26.248 | Malware |
| 195.110.43.159 | Malware |
| 204.11.56.48 | Malware |
| 196.245.247.17 | Malware |
| 103.27.61.222 | SQLi Attempt |

| | |
|---|---|
| 194.180.225.18 | Port Scan |
| 80.82.78.100 | Port Scan |
| 89.248.160.150 | Port Scan |
| 94.102.56.215 | Port Scan |
| 103.129.15.197 | Port Scan |
| 162.243.129.103 | Port Scan |
| 182.19.219.33 | Port Scan |
| 185.199.226.3 | Port Scan |
| 185.92.72.2 | Port Scan |
| 192.241.208.238 | Port Scan |
| 192.241.213.8 | Port Scan |
| 192.241.218.67 | Port Scan |
| 192.241.219.171 | Port Scan |
| 192.241.221.160 | Port Scan |
| 192.241.234.212 | Port Scan |
| 192.241.236.41 | Port Scan |
| 194.26.29.130 | Port Scan |
| 194.61.27.240 | Port Scan |
| 196.29.168.46 | Port Scan |
| 198.199.93.122 | Port Scan |
| 192.241.235.30 | Port Scan |
| 37.120.155.26 | Port Scan |
| 51.15.35.71 | Port Scan |
| 89.248.171.97 | Port Scan |
| 162.243.133.77 | Port Scan |
| 192.241.221.42 | Port Scan |
| 103.239.74.75 | Malware |
| 103.214.140.139 | Malware |
| 162.243.132.92 | Port Scan |
| 192.241.206.58 | Port Scan |
| 192.241.208.9 | Port Scan |
| 192.241.220.192 | Port Scan |
| 192.241.220.83 | Port Scan |

# 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.

- Roger Laya

# Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.30 18:52:55 -04'00'