13BCS20-00050-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 17 de Abril de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 09 de Abril y el miércoles 15 de Abril de 2020.

Falsificación de Registro o Identidad

8FFR20-00325-01 CSIRT ADVIERTE ACTIVACIÓN DE WEB BANCARIA FRAUDULENTA

Alerta de seguridad cibernética	8FFR20-00325-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 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 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/8ffr20-00325-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00325-01.pdf

8FFR20-00326-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00326-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 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/8ffr20-00326-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00326-01.pdf

8FFR20-00327-01 CSIRT ADVIERTE DE DOS SITIOS FRAUDULENTOS PARA ESTAFAS BANCARIAS

Alerta de seguridad cibernética	8FFR20-00327-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 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/8ffr20-00327-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00327-01.pdf

8FFR20-00328-01 CSIRT INFORMA DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00328-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociados a una IP que suplanta el sitio web oficial de Cencosud, 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/8ffr20-00328-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00328-01.pdf

8FFR20-00329-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00329-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociados a una IP que suplanta el sitio web oficial de Banco Itau, 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/8ffr20-00329-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00329-01.pdf

8FFR20-00330-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00330-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Abril de 2020
Última revisión	10 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 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/8ffr20-00330-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00330-01.pdf

8FFR20-00331-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00331-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 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 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/8ffr20-00331-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00331-01.pdf

8FFR20-00332-01 CSIRT ADVIERTE ACTIVACIÓN DE SITIO WEB BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00332-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 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 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/8ffr20-00332-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00332-01.pdf

8FFR20-00333-01 CSIRT ADVIERTE ACTIVACIÓN DE ONCE SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00333-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de once portales fraudulentos asociados a tres IPs que suplantan 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/8ffr20-00333-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00333-01.pdf

8FFR20-00334-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00334-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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/8ffr20-00334-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00334-01.pdf

8FFR20-00335-01 CSIRT ADVIERTE DE 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00335-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 tres IPs 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/8ffr20-00335-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00335-01.pdf

8FFR20-00336-01 CSIRT INFORMA DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00336-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 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/8ffr20-00336-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00336-01.pdf

8FFR20-00337-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00337-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 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/8ffr20-00337-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00337-01.pdf

8FPH20-00163-01 CSIRT ADVIERTE DE PHISHING POR VALIDACIÓN DE CUENTA DE CORREO

Alerta de seguridad cibernética	8FPH20-00163-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril 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 que supuestamente proviene del servicio de correos electrónicos Zimbra. El mensaje informa a quien recibe el correo, que la cuenta ha excedido el límite de cuota establecida por el administrador, y es posible que no pueda enviar o recibir correos hasta que vuelva a validar la cuenta. El atacante disponibiliza un enlace para realizar la validación. Si la víctima accede al enlace, ésta es dirigida a un sitio falso que imita el correo corporativo de Zimbra, donde se le solicita el nombre de usuario y contraseña, tras lo cual se expone al robo de credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00163-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00163-01.pdf

8FPH20-00164-01 CSIRT INFORMA PHISHING ACTIVO SOBRE DESCUENTO AUTOMÁTICO EN CUENTA

Alerta de seguridad cibernética	8FPH20-00164-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 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 aparenta provenir del Banco Scotiabank. El mensaje del correo informa a quien lo recibe que se realizó un descuento de $ 221.000 pesos, de manera automática, desde su cuenta por incumplimiento de un pago. El atacante dispone un enlace para supuestamente obtener más detalle del descuento. Si una persona selecciona el enlace, es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00164-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00164-01.pdf

8FPH20-00165-01 CSIRT ADVIERTE CAMPAÑAS DE PHISHING ASOCIADOS A DOS IP

Alerta de seguridad cibernética	8FPH20-00165-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha detectado dominios de suplantación de Banco Chile, Banco Scotiabank y Cencosud, que intentan engañar a los clientes utilizando técnicas de phishing. Los delincuentes intentan convencer a sus víctimas a través de correos electrónicos u otros medios, para que accedan a los sitios suplantados, con la finalidad de que los clientes entreguen sus credenciales de acceso a sus cuentas. La Ip [144.91.76.213], que intenta suplantar a la identidad Bancaria Scotiabank utilizando el dominio "online-cl.live", tiene la particularidad que al escribir cualquier subdominio utilizando caracteres alfa numéricos y un punto, es direccionado al sitio falso. La IP [178.159.36.139], que intenta suplantar la identidad del Banco de Chile y Cencosud, desde el 18 de marzo del 2020, está diariamente creando dominios falsos hasta. A la fecha de esta publicación, se han registrado 182 dominios. En todos los casos se ha utilizado la palabra covid-19 en el dominio, concepto asociado a la actual pandemia.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00165-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00165-01.pdf

8FPH20-00166-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING BANCARIO VIA WHATSAPP

Alerta de seguridad cibernética	8FPH20-00166-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 de Abril 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 Banco Estado habría detectado un dispositivo no frecuente (se asume que es para la realización de alguna transacción) y solicita a la personas que, para que la cuenta no sea suspendida debe verificar la información en el enlace adjunto disponible en el cierre del mensaje. Al seleccionarlo, la víctima es derivada a un sitio semejante al del banco, donde se le solicitan sus credenciales de acceso, y de esta forma el atacante obtiene sus datos.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00166-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00166-01.pdf

8FPH20-00167-01 CSIRT ADVIERTE DE PHISHING POR VALIDACIÓN EN CUENTA DE CORREO

Alerta de seguridad cibernética	8FPH20-00167-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 de Abril 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 que supuestamente proviene del servicio de correos electrónicos Zimbra.

El mensaje informa a quien recibe el correo, que la cuenta ha excedido el límite de cuota establecida por el administrador, y es posible que no pueda enviar o recibir correos hasta que vuelva a validar la cuenta. El atacante disponibiliza un enlace para realizar la validación. Si la víctima accede al enlace, ésta es dirigida a un sitio falso que imita el correo corporativo de Zimbra, donde se le solicita el nombre de usuario y contraseña, tras lo cual se expone al robo de credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00167-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00167-01.pdf

8FPH20-00168-01 CSIRT ADVIERTE DE PHISHING POR BONO DE AYUDA FAMILIAR COVID-19

Alerta de seguridad cibernética	8FPH20-00168-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Abril de 2020
Última revisión	07 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 Estado.

El mensaje del correo informa que está disponible un Bono Ayuda Familia Covid-19 de un monto de $80.000. El atacante disponibiliza enlaces en el correo para que las personas puedan consultar si son beneficiarios del bono, o para solicitar el Bono. De ingresar, las víctimas son dirigidas a un sitio falso del banco, donde se exponen al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00168-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00168-01.pdf

8FPH20-00169-01 CSIRT ADVIERTE PHISHING BANCARIO DE BENEFICIO DE PAGOS POR COVID-19

Alerta de seguridad cibernética	8FPH20-00169-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 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 Cencosud Scotiabank.

El mensaje del correo informa que, ante la contingencia nacional producto del Covid-19, el banco pone a su disposición de sus clientes alternativas de pagos. El mensaje informa de tres beneficias de acuerdo al tipo de cliente: uno para los clientes al día en el pago de sus tarjetas, otro para los clientes al día en el pago de sus créditos de consumo y un tercero para los clientes que presentan morosidad en el pago de su tarjera de crédito o crédito de consumo. El atacante disponibiliza un enlace para validar alguna alternativa, enlace a través del cual la víctima es dirigida a un sitio falso de Cencosud Scotiabank, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00169-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00169-01.pdf

8FPH20-00170-01 CSIRT ADVIERTE PHISHING POR CUENTA BANCARIA SUSPENDIDA

Alerta de seguridad cibernética	8FPH20-00170-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 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 Estado.

El mensaje del correo informa que existe un error, por ese motivo la cuenta se encuentra suspendida, ya que no se ha realizado el proceso de verificación de identidad. El atacante disponibiliza un enlace para que el cliente realice la verificación de su información. Al seleccionar el enlace, la persona 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/8fph20-00170-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00170-01.pdf

8FPH20-00171-01 CSIRT ADVIERTE PHISHING VÍA WHATSAPP CON OFERTA DE SERVICIO DE STREAMING

Alerta de seguridad cibernética	8FPH20-00171-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte de una campaña de phishing vía WhatsApp, proveniente supuestamente de la empresa de streaming Netflix.

El mensaje indica a quien lo recibe que, debido el impacto de COVID-19, ofrecerá gratis, por tres meses, una cuenta Premium. El atacante disponibiliza un enlace al final del mensaje. Al seleccionar el enlace, la persona es derivada a un sitio semejaste al de Netflix, donde se le solicita sus credenciales de acceso y se expone a la perdida de información personal y comercial.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00171-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00171-01.pd

8FPH20-00172-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR AVANCE EN EFECTIVO

Alerta de seguridad cibernética	8FPH20-00172-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 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 aparenta provenir del Banco Scotiabank.

El mensaje del correo informa que es factible obtener un avance en efectivo, de manera rápida y fácil, que es posible pagar hasta en 48 cuotas. El atacante disponibiliza dos enlaces: uno de ellos, denominado “Hazte Cliente”, de ser seleccionado envía a la persona al sitio oficial del Banco. Or el contrario, el segundo enlace, “Acceso Scotiabank”, direcciona a la víctima a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00172-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00172-01.pdf

8FPH20-00173-01 CSIRT ADVIERTE DE PHISHING POR BLOQUEA DE CUENTA BANCARIA

Alerta de seguridad cibernética	8FPH20-00173-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 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 Estado.

El mensaje del correo informa que se realizó un mantenimiento en los servicios del banco: Caja Vecina, ServiEstado y aplicaciones. Durante esa acción, se habría descubierto un supuesto un error en la cuenta. Como consecuencia, se informa a la potencial víctima que se procedió al bloqueo de la cuenta. Para poder corregir la situación, el atacante disponibiliza un enlace para que el cliente realice la verificación de su información. Al seleccionar el enlace, la persona es dirigida a un sitio web semejante al del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00173-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00173-01.pdf

8FPH20-00174-01 CSIRT ADVIERTE PHISHING POR ACTIVIDAD NO FRECUENTE EN DISPOSITIVO

Alerta de seguridad cibernética	8FPH20-00174-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 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 WhatsApp supuestamente proveniente del Banco Estado. El mensaje informa a quien lo recibe que debe verificar su cuenta para evitar que sea suspendida, ya que -se desprende del texto- se registró actividad desde un dispositivo no frecuente del usuario. El atacante disponibiliza un enlace para que el cliente realice la verificación de su información, el cual, al ser seleccionado, dirige a la persona a un sitio web semejante al del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00174-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00174-01.pdf

8FPH20-00175-01 CSIRT ADVIERTE DE PHISHING QUE PROMUEVE USO DE SERVICIOS BANCARIOS ONLINE

Alerta de seguridad cibernética	8FPH20-00175-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 Chile. El mensaje busca que los colaboradores, clientes y proveedores del banco utilicen los servicios en línea de la entidad a través del enlace malicioso que se ofrece en el cuerpo del correo. Para engañar a sus víctimas los atacantes utilizan como argumento el compromiso con la salud de sus clientes y ofrecen los servicios de las plataformas digitales como alternativa a la asistencia a las sucursales en este contexto de emergencia sanitaria. Si las personas seleccionan el enlace, serán dirigidos a un sitio web semejante al del banco, donde se exponen al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00175-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00175-01.pdf

8FPH20-00176-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING POR VALIDACIÓN DE CUENTA DE CORREO

Alerta de seguridad cibernética	8FPH20-00176-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 de Abril 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 que usurpa la identidad de la mesa de ayuda del administrador de correos de Zimbra.

El asunto del mensaje, marcado como urgente, señala que por un error en la sincronización con Zimbra, y para evitar la pérdida de los contactos y mensajes del correo electrónico, es necesario validar la cuenta a través de un enlace dispuesto en el cuerpo del correo.

El objetivo es persuadir a las potenciales víctimas para ingresar al enlace malicioso adjunto en el falso correo corporativo y capturar información relevante, como el nombre de usuario y la contraseña.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00176-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00176-01.pdf

8FPH20-00177-01 CSIRT ADVIERTE PHISHING QUE PROMUEVE CANALES DIGITALES BANCARIOS

Alerta de seguridad cibernética	8FPH20-00177-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 Chile. El mensaje busca que los colaboradores, clientes y proveedores del banco utilicen los servicios en línea de la entidad a través del enlace malicioso que se ofrece en el cuerpo del correo. Para engañar a sus víctimas los atacantes utilizan como argumento el compromiso con la salud de sus clientes y ofrecen los servicios de las plataformas digitales como alternativa a la asistencia a las sucursales en este contexto de emergencia sanitaria.
Si las personas seleccionan el enlace, serán dirigidos a un sitio web semejante al del banco, donde se exponen al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00177-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00177-01.pdf

8FPH20-00178-01 CSIRT ADVIERTE PHISHING POR INCONVENIENTE EN DISPOSITIVO DE SEGURIDAD

Alerta de seguridad cibernética	8FPH20-00178-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 aparenta provenir del Banco Scotiabank. El mensaje intenta persuadir a las personas para utilizar un enlace malicioso adjunto en el cuerpo del correo.Quien recibe el correo es informado sobre la detección de un inconveniente con su dispositivo de seguridad, por lo que se requiere su sincronización de forma inmediata. El mensaje advierte de un tiempo límite para realizar la acción -48 horas desde recibido el correo- de lo contrario la cuenta podría ser bloqueada, lo que podría generar presión en la decisión de la víctima para ingresar a los enlaces disponibles en el correo para realizar la gestión de sincronizar el dispositivo. Si la persona utiliza el enlace, es redirigido a un sitio semejante al del banco donde se expone al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00178-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00178-01.pdf

8FPH20-00179-01 CSIRT ADVIERTE PHISHING BANCARIO PARA USO DE SERVICIOS EN LÍNEA

Alerta de seguridad cibernética	8FPH20-00179-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 Chile. El mensaje busca que los colaboradores, clientes y proveedores del banco utilicen los servicios en línea de la entidad a través del enlace malicioso que se ofrece en el cuerpo del correo. Para engañar a sus víctimas los atacantes utilizan como argumento el compromiso con la salud de sus clientes y ofrecen los servicios de las plataformas digitales como alternativa a la asistencia a las sucursales en este contexto de emergencia sanitaria. Si las personas seleccionan el enlace, serán dirigidos a un sitio web semejante al del banco, donde se exponen al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00179-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00179-01.pdf

8FPH20-00180-01 CSIRT ADVIERTE PHISHING VÍA WHATSAPP CON FALSA OFERTA DE SUPERMERCADO

Alerta de seguridad cibernética	8FPH20-00180-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Abril de 2020
Última revisión	15 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 WhatsApp, supuestamente proveniente del supermercado Líder. Los atacantes tratan de persuadir a las personas para utilizar el enlace disponible en el cuerpo del mensaje. El mensaje informa que durante el período que dura la cuarentena, supermercados Líder y Líder Express regalarán cupones de $100.000 pesos y disponibilizan un enlace para obtener el cupón. Si una persona utiliza el enlace es derivada a una encuesta. Una vez que responde la encuesta debe reenviar el mensaje de WhatsApp. Posteriormente se le solicitan un correo y clave y finalmente una tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00180-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00180-01.pdf

9VSA20-00174-01 CSIRT COMPARTE INFORMACIÓN ENTREGADA POR GOOGLE PARA EL NAVEGADOR CHROME

Alerta de seguridad cibernética	9VSA20-00174-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril de 2020

Vulnerabilidad

CVE-2020-6423
CVE-2020-6430
CVE-2020-6431
CVE-2020-6432
CVE-2020-6433
CVE-2020-6434
CVE-2020-6435
CVE-2020-6436
CVE-2020-6437
CVE-2020-6438
CVE-2020-6439
CVE-2020-6440
CVE-2020-6441
CVE-2020-6442
CVE-2020-6443
CVE-2020-6444
CVE-2020-6445
CVE-2020-6446
CVE-2020-6447
CVE-2020-6448
CVE-2020-6454
CVE-2020-6455
CVE-2020-6456

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00174-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00174-01.pdf

9VSA20-00175-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR VMWARE

Alerta de seguridad cibernética	9VSA20-00175-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Abril de 2020
Última revisión	11 de Abril de 2020

Vulnerabilidad

CVE-2020-3952

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMWare referente a una vulnerabilidad críticas que afecta a uno de sus productos. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00175-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00175-01.pdf

9VSA20-00176-01 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA THUNDERBIRD

Alerta de seguridad cibernética	9VSA20-00176-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 de Abril de 2020

Vulnerabilidad

CVE-2020-6819
CVE-2020-6820
CVE-2020-6821
CVE-2020-6822
CVE-2020-6825

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Mozilla referente a múltiples vulnerabilidades críticas que afectan a Mozilla Thunderbird. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00176-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00176-01.pdf

9VSA20-00177-01 CSRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS DE PALOALTO

Alerta de seguridad cibernética	9VSA20-00177-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Abril de 2020
Última revisión	13 de Abril de 2020

Vulnerabilidad

CVE-2020-1984
CVE-2020-1992
CVE-2020-1990
CVE-2020-1987
CVE-2020-1989
CVE-2020-1988
CVE-2020-1985
CVE-2020-1986
CVE-2020-1991
CVE-2020-1978
PAN-SA-2020-0002
CVE-2018-20685
CVE-2019-6109
CVE-2019-6111

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00177-01/
https://www.csirt.gob.cl/media/2020/04/9VSA-00177-01.pdf

9VSA20-00178-01 CSIRT COMPARTE ACTUALIZACIONES PARA VMWARE VREALIZE LOG INSIGHT

Alerta de seguridad cibernética	9VSA20-00178-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Abril de 2020
Última revisión	14 de Abril de 2020

Vulnerabilidad

CVE-2020-3953

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMware referente a dos vulnerabilidades que afectan a VMware vRealize Log Insight. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00178-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00178-01.pdf

9VSA20-00179-01 CSIRT COMPARTE ACTUALIZACIONES DE PRODUCTOS MICROSOFT

Alerta de seguridad cibernética	9VSA20-00179-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Abril de 2020
Última revisión	04 de Abril de 2020

Vulnerabilidad

VE-2020-0929	CVE-2020-0930	CVE-2020-0973
CVE-2020-0931	CVE-2020-0933	CVE-2020-0975
CVE-2020-0932	CVE-2020-0935	CVE-2020-0976
CVE-2020-0974	CVE-2020-0937	CVE-2020-0977
CVE-2020-0699	CVE-2020-0939	CVE-2020-0978
CVE-2020-0760	CVE-2020-0945	CVE-2020-0979
CVE-2020-0821	CVE-2020-0946	CVE-2020-0980
CVE-2020-0835	CVE-2020-0947	CVE-2020-0982
CVE-2020-0906	CVE-2020-0952	CVE-2020-0987
CVE-2020-0920	CVE-2020-0954	CVE-2020-0991
CVE-2020-0923	CVE-2020-0955	CVE-2020-1002
CVE-2020-0924	CVE-2020-0961	CVE-2020-1005
CVE-2020-0925	CVE-2020-0962	CVE-2020-1007
CVE-2020-0926	CVE-2020-0971	CVE-2020-1016
CVE-2020-0927	CVE-2020-0972	CVE-2020-1018

Vulnerabilidades adicionales informadas

ADV200006	CVE-2020-0917	CVE-2020-0994
CVE-2020-0687	CVE-2020-0918	CVE-2020-0995
CVE-2020-0796	CVE-2020-0919	CVE-2020-0996
CVE-2020-0907	CVE-2020-0934	CVE-2020-0999
CVE-2020-0910	CVE-2020-0936	CVE-2020-1000
CVE-2020-0938	CVE-2020-0940	CVE-2020-1001
CVE-2020-0948	CVE-2020-0942	CVE-2020-1003
CVE-2020-0949	CVE-2020-0943	CVE-2020-1004
CVE-2020-0950	CVE-2020-0944	CVE-2020-1006
CVE-2020-0965	CVE-2020-0953	CVE-2020-1008
CVE-2020-0967	CVE-2020-0956	CVE-2020-1009

CVE-2020-0968	CVE-2020-0957	CVE-2020-1011
CVE-2020-0969	CVE-2020-0958	CVE-2020-1014
CVE-2020-0970	CVE-2020-0959	CVE-2020-1015
CVE-2020-1020	CVE-2020-0960	CVE-2020-1017
CVE-2020-1022	CVE-2020-0964	CVE-2020-1019
CVE-2020-0784	CVE-2020-0966	CVE-2020-1026
CVE-2020-0794	CVE-2020-0981	CVE-2020-1027
CVE-2020-0888	CVE-2020-0983	CVE-2020-1029
CVE-2020-0889	CVE-2020-0984	CVE-2020-1049
CVE-2020-0895	CVE-2020-0985	CVE-2020-1050
CVE-2020-0899	CVE-2020-0988	CVE-2020-1094
CVE-2020-0900	CVE-2020-0992	
CVE-2020-0913	CVE-2020-0993	

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft en su reporte mensual de actualizaciones correspondiente a abril de 2020, parchando 45 vulnerabilidades en sus softwares clasificando a 4 de ellas como críticas y 41 como importantes, además se informa de 70 vulnerabilidades adicionales al reporte mensual, 16 de ellas clasificadas como críticas y 54 como importantes.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00179-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00179-01.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
3.132.217.113	DDoS
158.69.162.108	Port Scan
51.79.8.5	DDoS
162.243.130.239	Port Scan
94.23.23.90	Port Scan
192.241.239.160	Port Scan
192.241.239.155	Port Scan
45.143.220.35	Port Scan
170.130.187.42	Port Scan
192.241.239.24	Port Scan
80.82.78.100	DDoS

94.237.42.60	DDoS
80.82.77.245	DDoS
167.172.132.237	Port Scan
162.243.130.14	Port Scan
192.241.203.41	Port Scan
64.251.51.98	Port Scan
192.254.224.60	Phishing
192.241.237.188	Port Scan
162.243.129.42	Port Scan
162.243.133.193	Port Scan
103.253.42.38	Port Scan
45.143.220.50	Port Scan
78.31.67.32	Port Scan
23.248.188.6	Port Scan
51.77.124.170	Port Scan
192.241.237.77	Port Scan
162.243.132.213	Port Scan
185.198.56.213	Port Scan
92.63.196.13	Port Scan
193.32.163.112	Port Scan
69.10.58.162	Port Scan
107.167.21.82	Port Scan
45.143.220.214	Port Scan
37.49.230.32	Port Scan
51.79.57.12	Port Scan
144.217.82.79	Port Scan
162.243.132.162	Port Scan
163.172.9.33	Port Scan
77.247.109.68	Port Scan
62.171.186.137	Port Scan
103.133.109.41	Port Scan
88.218.17.103	Port Scan
195.231.0.27	Port Scan
171.225.251.80	Port Scan
93.174.93.91	Port Scan
193.142.146.88	Port Scan
162.243.132.42	Port Scan
162.243.128.96	Port Scan
83.97.20.34	Port Scan
192.241.237.69	Port Scan
162.243.132.142	Port Scan

162.243.133.182	Port Scan
162.243.132.38	Port Scan
45.143.220.101	Port Scan
190.120.59.203	Port Scan
80.82.64.42	Port Scan
95.168.171.165	Port Scan
89.203.137.87	Port Scan
79.124.62.55	Port Scan
98.108.67.80	Port Scan
193.32.161.117	Port Scan
185.30.166.150	Port Scan
192.241.237.216	Port Scan
51.68.143.219	Port Scan
192.241.238.18	Port Scan
192.241.239.20	Port Scan
192.241.239.126	Port Scan
103.145.12.53	Port Scan
192.241.238.169	Port Scan
162.243.133.174	Port Scan
95.168.165.82	Port Scan
192.241.238.130	Port Scan
162.243.129.150	Port Scan
98.181.158.70	Port Scan
162.243.129.187	Port Scan
192.241.237.170	Port Scan
162.243.129.46	Port Scan
162.243.132.59	Port Scan
103.145.12.26	Port Scan
103.145.13.4	Port Scan
59.56.78.144	Port Scan
77.81.191.142	Port Scan
157.245.133.106	Port Scan
192.241.239.69	Port Scan
192.241.238.218	Port Scan
192.241.238.175	Port Scan
62.171.182.146	Port Scan
62.210.91.225	Port Scan
45.143.220.123	Port Scan
192.241.238.144	Port Scan
163.172.63.23	Port Scan
192.241.238.208	Port Scan

45.143.220.235	Port Scan
192.241.200.71	Port Scan
45.55.55.17	Port Scan
103.145.13.3	Port Scan
45.79.82.183	Port Scan
192.241.234.142	Port Scan
61.153.110.89	DDoS
103.46.138.52	DDoS
92.114.17.214	DDoS
185.136.167.213	Port Scan
134.122.75.66	Port Scan
198.144.154.56	DDoS
27.78.14.83	Port Scan
116.105.216.179	Port Scan
185.153.198.227	DDoS
50.7.206.2	DDoS
195.3.146.114	DDoS
37.49.226.4	DDoS
167.172.152.143	DDoS
64.227.24.112	DDoS
185.153.198.227	DDoS
67.205.154.203	DDoS
157.245.93.85	DDoS
144.217.214.100	DDoS
81.219.238.175	DDoS
159.65.154.48	DDoS
167.99.229.185	DDoS
45.143.220.234	Port Scan
185.117.118.91	Port Scan
144.217.10.231	Port Scan
89.163.153.41	Port Scan
95.168.167.140	Port Scan
37.49.226.250	Port Scan
94.158.244.113	Port Scan
93.174.93.213	Port Scan
23.231.25.234	Port Scan
157.230.47.57	Port Scan
209.188.21.99	Port Scan
23.95.0.119	Port Scan
85.93.20.248	Port Scan
167.172.207.15	Port Scan

139.162.205.20	Port Scan
49.50.85.116	Port Scan
192.241.236.76	Port Scan
165.22.52.20	Port Scan
146.185.141.95	Port Scan
178.159.36.139	Phishing
195.35.201.14	Port Scan
195.35.245.30	Port Scan
212.178.154.174	Port Scan
213.34.163.254	Port Scan
212.178.135.62	Port Scan
213.34.171.254	Port Scan
45.143.220.54	Port Scan
181.214.91.28	Port Scan
94.46.223.163	Port Scan
128.14.140.82	Port Scan
140.238.167.41	Port Scan
195.231.8.97	Port Scan
51.159.59.122	Port Scan
213.233.179.194	Port Scan
103.145.12.68	Port Scan
162.243.134.25	Port Scan
201.214.158.191	Malware
146.83.205.200	Malware
159.65.149.158	Phishing
185.53.88.103	Port Scan
198.98.62.43	Port Scan
51.15.19.223	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.

- Rodrigo Ostaloza: Twitter: @NegroOstolaza
- Patricio Jofré. Twitter: @CasperNear
- Eduardo Riveros. Twitter: @RiverosRoca
- Denny. Twitter: Twitter: @BrujtO

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: 2020.04.16 19:13:17 -04'00'