13BCS20-00049-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 10 de Abril de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 02 de Abril y el miércoles 08 de Abril de 2020.

Falsificación de Registro o Identidad

8FFR20-00300-01 CSIRT ADVIERTE ACTIVACIÓN DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00300-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 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 un 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/8ffr20-00300-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00300-01.pdf

8FFR20-00301-01 CSIRT ADVIERTE ACTIVACIÓN DE DOS SITIOS FRAUDULENTES PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad cibernética	8FFR20-00301-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 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 una IP que suplantan el sitio web oficial de Banco de Chile, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00301-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00301-01.pdf

8FFR20-00302-01 CSIRT INFORMA ACTIVACIÓN DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00302-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 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/8ffr20-00302-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00302-01.pdf

8FFR20-00303-01 CSIRT ADVIERTE ACTIVACIÓN DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00303-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 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/8ffr20-00303-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00303-01.pdf

8FFR20-00304-01 CSIRT ADVIERTE ACTIVACIÓN DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad cibernética	8FFR20-00304-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de la tarjeta 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/8ffr20-00304-01/
https://www.csirt.gob.cl/media/2020/04/8FFR-00304-01.pdf

8FFR20-00305-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00305-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 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/8ffr20-00305-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00305-01.pdf

8FFR20-00306-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS, UNO CON URL COVID19

Alerta de seguridad cibernética	8FFR20-00306-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 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 Chile, el que podría servir para robar credenciales de usuarios de esa entidad. La URL de uno de los sitios utiliza el término covid-19.

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/8ffr20-00306-01/

https://www.csirt.gob.cl/media/2020/04/8FFR-00306-01.pdf

8FFR20-00307-01 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00307-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 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 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/8ffr20-00307-01/
https://www.csirt.gob.cl/media/2020/04/8FFR-00307-01.pdf

8FFR20-00308-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

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

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha 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/8ffr20-00308-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00308-01.pdf

8FFR20-00309-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00309-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Abril de 2020
Última revisión	04 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 la tarjeta 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/8ffr20-00309-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00309-01.pdf

8FFR20-00310-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00310-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Abril de 2020
Última revisión	04 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/8ffr20-00310-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00310-01.pdf

8FFR20-00311-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00311-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Abril de 2020
Última revisión	04 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/8ffr20-00311-01-csirt-advierte-de-dos-portales-bancarios-fraudulentos/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00311-01.pdf

8FFR20-00312-01 CSIRT ADVIERTE DE UN SITIO BANCARIOS FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00312-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Abril de 2020
Última revisión	04 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 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/8ffr20-00312-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00312-01.pdf

8FFR20-00313-01 CSIRT ADVIERTE LA ACTIVACIÓN DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00313-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Cencosud, el que podría servir para robar credenciales de usuarios de esa entidad. Los portales utilizan el nombre de la campaña "quédate en casa", asociado a covid-19.

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/8ffr20-00313-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00313-01.pdf

8FFR20-00314-01 CSIRT ADVIERTE DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00314-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), 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/8ffr20-00314-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00314-01.pdf

8FFR20-00315-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00315-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), 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/8ffr20-00315-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00315-01.pdf

8FFR20-00316-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00316-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), ha identificado la activación 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/8ffr20-00316-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00316-01.pdf

8FFR20-00317-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00317-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan 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/8ffr20-00317-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00317-01.pdf

8FFR20-00318-01 CSIRT INFORMA DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00318-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), 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/8ffr20-00318-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00318-01.pdf

8FFR20-00319-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00319-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
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), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00319-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00319-01.pdf

8FFR20-00320-01 CSIRT informa de dos sitios web bancarios FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00320-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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/8ffr20-00320-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00320-01.pdf

8FFR20-00321-01 CSIRT ADVIERTE LA ACTIVACIÓN DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00321-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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 dos 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/8ffr20-00321-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00321-01.pdf

8FFR20-00322-01 CSIRT ADVIERTE ACTIVACIÓN DE DOS SITIOS BANCARIOS PARA FRAUDES

Alerta de seguridad cibernética	8FFR20-00322-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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 una IP 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/8ffr20-00322-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00322-01.pdf

8FFR20-00323-01 CSIRT INFORMA DE LA ACTIVACIÓN DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00323-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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 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/8ffr20-00323-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00323-01.pdf

8FFR20-00324-01 CSIRT ADVIERTE ACTIVACIÓN DE SITIO FRAUDULENTO DE TARJETA DE CRÉDITO

Alerta de seguridad cibernética	8FFR20-00324-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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 la tarjeta 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/8ffr20-00324-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00324-01.pdf

8FPH20-00152-01 CSIRT ADVIERTE PHISHING BANCARIO POR AUMENTO DE CUPO EN LÍNEA DE CRÉDITO

Alerta de seguridad cibernética	8FPH20-00152-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 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 BCI.

El mensaje del correo ofrece un aumento de cupo en la línea de crédito por $500.000 pesos. La oferta indica que si la persona solicita el aumento, automáticamente participará en el sorteo de 60 televisores LED Samsung de 55", 100 PLAY STATION 4 y 250 Motorola E5 16GB. Si una persona selecciona el enlace aprobando el abono, esta será dirigida a un sitio semejante al del banco, donde se expone al robo de sus credenciales bancarias.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00152-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00152-01.pdf

8FPH20-00153-01 CSIRT ADVIERTE PHISHING SOBRE FONDOS DE AYUDA POR LA PANDEMIA DE COVID-19

Alerta de seguridad cibernética	8FPH20-00153-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo de 2020

Resumen

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

El mensaje del correo indica a quien lo recibe que ha sido seleccionado por Microsoft para recibir fondos de ayuda producto de la pandemia del Coronavirus. Para obtener más información sobre cómo supuestamente obtener estos recursos, los atacantes solicitan de la potencial víctima el envío de un código adjunto, en este ejemplo, es el LD66271, el cual debe ser enviado a una casilla de correo.

Enlace:
https://www.csirt.gob.cl/alertas/8fph20-00153-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00153-01.pdf

8FPH20-00154-01 CSIRT IDENTIFICÓ PHISHING POR SUSPENSIÓN DE SERVICIO STREAMING

Alerta de seguridad cibernética	8FPH20-00154-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Abril de 2020
Última revisión	05 de Abril de 2020

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de la aplicación de mensajería instantánea Telegram. El mensaje informa que la suscripción a Netflix se ha suspendido. El mensaje solicita a la víctima que para volver a recibir el servicio debe actualizar su forma de pago, para lo cual dispone de un enlace por medio del cual se activa el fraude.
Enlace:
https://www.csirt.gob.cl/alertas/8fph20-00154-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00154-01.pdf

8FPH20-00155-01 CSIRT ADVIERTE PHISHING POR CUENTA SUSPENDIDA EN SERVICIO DE STREAMING

Alerta de seguridad cibernética	8FPH20-00155-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Abril de 2020
Última revisión	06 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 aparentemente proviene del servicio de streaming Netflix.
El mensaje informa que la cuenta del usuario se encuentra suspendida y debe ser actualizada la información para corregir el problema. El atacante dispone un enlace en el mensaje para ser derivado a un sitio falso que imita a la web oficial del servicio de streaming, en la cual le solicitan ingresar sus credenciales para iniciar una sesión.
Enlace:
https://www.csirt.gob.cl/alertas/8fph20-00155-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00155-01.pdf

8FPH20-00156-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING BANCARIO POR COVID-19

Alerta de seguridad cibernética	8FPH20-00156-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Marzo de 2020
Última revisión	29 de Marzo de 2020

Resumen

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

El mensaje del correo informa que el banco, tomando conciencia relacionada a la pandemia de COVID-19 que está afectando a cientos de chilenos, ha optado por reprogramar sus pagos de préstamos, tarjetas de crédito, créditos hipotecarios, crecidos vehiculares, créditos por salud, entre otros servicios que presta a sus clientes. El atacante disponibiliza un enlace para ingresar supuestamente al portal y reprogramar las deudas, pero si una persona selecciona el enlace será dirigido a un sitio semejante al del banco, donde se expone al robo de sus credenciales

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00156-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00156-01.pdf

8FPH20-00157-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR DATOS INVÁLIDOS DE CLIENTES

Alerta de seguridad cibernética	8FPH20-00157-01
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 falso que aparenta provenir del Banco ITAU.

El mensaje del correo informa que producto de una actualización de los sistemas se detectó un error en la cuenta, encontrándose inválidos los siguientes datos; dirección, número telefónico y correo electrónico, por ese motivo el banco procedo con el bloqueo de la cuenta. El atacante disponibiliza un enlace supuestamente para realizar el proceso de desbloqueo, pero al seleccionar dicho enlace es dirigido a un sitio semejante al del banco, donde se expone al robo de sus credenciales

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00157-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00157-01.pdf

8FPH20-00158-01 CSIRT ADVIERTE PHISHING POR SUPUESTOS ARCHIVOS COMPARTIDOS

Alerta de seguridad cibernética	8FPH20-00158-01
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 del Gobierno de Chile, CSIRT, advierte sobre una campaña de phishing.

El mensaje del correo escrito en inglés, informa que una persona llamada Michaela Lancu compartió algunos archivos con la persona que recibe el correo. El atacante facilita un enlace a la potencial víctima, supuestamente de los servicios Onedriver, empresa de almacenamiento de archivos de Microsoft. Si una persona selecciona el enlace es direccionada a un sitio falso de Microsoft donde son solicitadas sus credenciales de acceso, exponiéndose a la captura de esa información.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00158-01-csirt-advierte-phishing-por-supuestos-archivos-compartidos/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00158-01.pdf

8FFR20-00159-01 CSIRT ADVIERTE SOBRE PHISHING DE SUPERMERCADOS VÍA WHATSAAP

Alerta de seguridad cibernética	8FPH20-00159-01
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), ha identificado una campaña de phishing vía WhatsApp, indicando que los supermercados Jumbo y Santa Isabel invitan a participar por una Gift Card de 200.000 pesos a quienes reciben el mensaje.

El atacante disponibiliza un vínculo para que la víctima participe en supuesta promoción. De presionar el enlace, la víctima es direccionada a un sitio semejante al de los supermercados, dónde se le invita a completar una encuesta a través de la cual se le solicitan datos personales (correo electrónico, nombre, apellidos, región, comuna, número telefónico, dirección, fecha de nacimiento y cedula de identidad). Al concluir las preguntas, la víctima es direccionada a sitios de Adware o publicidad.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00159-01/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00159-01.pdf

8FPH20-00160-01 CSIRT ADVIERTE DE SMISHING BANCARIO POR CUENTA DESVINCULADA

Alerta de seguridad cibernética	8FPH20-00160-01
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 SMiShing a través de un mensaje de texto que intenta engañar a los usuarios del Banco ITAU.

El atacante envía un mensaje señalando a quien lo recibe, que su cuenta bancaria de se encuentra desvinculada en el sistema. Para solucionar el inconveniente, se deben actualizar los datos en un enlace adjunto. De seleccionar el enlace, la víctima es dirigida a un sitio semejante al del Banco. De esta forma el atacante captura las credenciales de la persona.

CSIRT agradece la colaboración de Nicolle Bravo, (@NicolleABG) quien informó de este SMiShing a través de nuestro twitter. Y recordamos a todos quienes siguen nuestros informes que para reportar un incidente, lo pueden hacer en el formulario de nuestro sitio web www.csirt.gob.cl o al teléfono +(562) 2486 3850, las 24 horas del día.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00160-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00160-01.pdf

8FPH20-00161-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR MANTENIMIENTO DE PATAFORMAS

Alerta de seguridad cibernética	8FPH20-00161-01
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 falso que aparenta proviene del Banco Estado. El mensaje del correo informa que el Banco Estado a realizado un mantenimiento en sus plataformas de Servicios, como Caja Vecina, ServiEstado y otras App. Durante ese procedimiento, supuestamente se encontró un error en la cuenta de la potencial víctima. Debido a esto, el mensaje indica que por seguridad se ha procedido al bloqueo de la cuenta. Para facilitar la activación de la cuenta el atacante disponibiliza un enlace para ingresar a un portal que imita al del banco, donde la persona se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00161-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00161-01.pdf

8FPH20-00162-01 SE ADVIERTE PHISHING DE SUPUESTA EXTORSIÓN POR VISITAR WEB PORNOGRÁFICA

Alerta de seguridad cibernética	8FPH20-00162-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Abril de 2020
Última revisión	08 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 en inglés.

El mensaje informa que un atacante supuestamente logró obtener acceso a la pantalla y cámara web de quien recibe el correo, y con un software logra reunir todos los contactos de Messenger, Facebook y la cuenta de la persona.

En el mensaje se le indica al receptor del correo que fue grabado mientras visitaba un sitio con pornografía. Luego, el atacante señala que con un software que descargó en el equipo de la víctima pudo grabarla utilizando la cámara web. Bajo la amenaza de exponer el video grabado a sus contactos, como amigos, familiares y colegas, el atacante demanda el pago de $2.000 dólares, el cual no es negociable y el que debe ser cancelado en Bitcoins dentro de 24 horas. De acuerdo a lo que indica el atacante, el correo posee un pixel de rastreo con el cual ya sabe que ha leído mensaje.

El mensaje de extorsión finaliza desafiando a la víctima, indicándole que si desea tener evidencia del video solo debe responder “Yes» y le serán enviadas copias de la grabación a 5 de sus contactos.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00162-01/

https://www.csirt.gob.cl/media/2020/04/8FPH20-00162-01.pdf

9VSA20-00168-01 CSIRT COMPARTE ACTUALIZACIONES PARA EL SERVIDO HTTP DE APACHE

Alerta de seguridad cibernética	9VSA20-00168-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 de Abril de 2020

Vulnerabilidad

CVE-2020-1927

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Apache referente a dos vulnerabilidades que afectan a su servidor HTTP. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00168-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00168-01.pdf

9VSA20-00169-01 CSIRT COMPARTE INFORMACIÓN SOBRE UNA VULNERABILIDAD ENTREGADA POR ZOOM

Alerta de seguridad cibernética	9VSA20-00169-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Abril de 2020
Última revisión	02 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Zoom referente a una vulnerabilidad que afecta a su producto.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00169-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00169-01.pdf

9VSA20-00170-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR AVAST

Alerta de seguridad cibernética	9VSA20-00170-01

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 de Abril de 2020

Vulnerabilidad

CVE-2020-10868
CVE-2020-10867
CVE-2020-10866
CVE-2020-10865
CVE-2020-10864
CVE-2020-10863
CVE-2020-10862
CVE-2020-10861
CVE-2020-10860

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00170-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00170-01.pdf

9VSA20-00171-01 CSIRT COMPARTE INFORMACIÓN ENTREGADA POR GRAFANA

Alerta de seguridad cibernética	9VSA20-00171-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Abril de 2020
Última revisión	03 de Abril de 2020

Vulnerabilidad

CWE-79

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/9vsa20-00171-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00171-01.pdf

9VSA20-00172-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR MOZILLA

Alerta de seguridad cibernética	9VSA20-00172-01

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

CVE-2020-6819
CVE-2020-6820

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00172-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00172-01.pdf

9VSA20-00173-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR MOZILLA PARA FOREFOX Y FIREFOX ESR

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	04 de Abril de 2020
Última revisión	04 de Abril de 2020

Vulnerabilidad

CVE-2020-6821
CVE-2020-6822
CVE-2020-6823
CVE-2020-6824
CVE-2020-6825
CVE-2020-6826
CVE-2020-6827
CVE-2020-6828
CVE-2020-6821

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 sus navegadores Firefox y Firefox ESR. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00173-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00173-01.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante las pasadas dos semanas por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad:

IoC	Motivo
162.243.133.68	Port Scan
37.49.226.3	Port Scan
162.243.128.14	Port Scan
192.241.238.216	Port Scan
192.241.238.209	Port Scan
192.241.239.9	Port Scan
45.79.114.128	Port Scan
139.162.126.103	Port Scan
110.232.250.146	Port Scan
66.212.30.236	Port Scan
175.194.140.249	Port Scan
209.148.131.37	Port Scan
192.241.239.219	Port Scan
67.231.208.173	Port Scan
196.52.84.8	Port Scan
140.238.224.56	Port Scan
46.105.112.86	Port Scan
198.199.109.76	Port Scan
37.139.30.95	Malware
159.89.174.206	Port Scan
80.82.77.42	Port Scan
51.159.0.23	Port Scan
162.243.128.48	Port Scan
192.241.237.128	Port Scan
162.243.129.245	Port Scan
162.243.129.163	Port Scan
162.243.133.119	Port Scan
192.241.239.53	Port Scan
192.241.237.136	Port Scan
192.241.239.156	Port Scan
162.243.128.180	Port Scan
162.243.133.172	Port Scan
162.243.133.13	Port Scan
162.243.133.98	Port Scan

162.243.129.170	Port Scan
192.241.239.46	Port Scan
162.243.133.69	Port Scan
192.241.237.216	Port Scan
51.158.31.243	Port Scan
162.243.129.211	Port Scan
51.159.0.30	Port Scan
89.163.225.183	Port Scan
89.163.224.164	Port Scan
162.243.131.206	Port Scan
162.243.128.209	Port Scan
123.253.88.59	Port Scan
162.243.134.36	Port Scan
162.243.133.15	Port Scan
162.243.129.133	Port Scan
162.243.130.10	Port Scan
192.241.239.56	Port Scan
173.0.56.34	Port Scan
185.153.198.243	Port Scan
162.243.130.84	Port Scan
192.241.237.127	Port Scan
103.114.106.228	Port Scan
45.13.93.90	Port Scan
51.83.217.97	Port Scan
118.99.91.73	Port Scan
80.211.241.152	Port Scan
144.91.69.220	Port Scan
162.243.132.34	Port Scan
162.243.131.10	Port Scan
212.83.170.85	Port Scan
162.243.134.15	Port Scan
51.89.235.112	Port Scan
162.243.134.31	Port Scan
162.243.129.170	Port Scan
192.241.237.137	Port Scan
182.252.135.34	Port Scan
162.243.131.153	Port Scan
192.241.238.217	Port Scan
162.243.133.99	Port Scan
122.155.169.223	Port Scan
192.241.226.27	Port Scan

192.241.235.76	Port Scan
192.241.238.84	Port Scan
162.243.129.112	Port Scan
162.243.128.120	Port Scan
104.221.228.26	Port Scan
185.153.198.203	Port Scan
104.221.228.26	Port Scan
162.243.131.8	Port Scan
162.243.128.18	Port Scan
162.243.133.187	Port Scan
45.143.220.249	Port Scan
162.243.131.42	Port Scan
122.114.50.108	DDoS
51.15.114.117	DDoS
185.137.234.22	DDoS
80.82.77.42	DDoS
92.118.37.86	DDoS
118.184.253.2	DDoS
87.119.195.44	Port Scan
139.178.88.75	Port Scan
147.203.238.18	Port Scan
104.194.10.157	Port Scan
104.194.8.73	Port Scan
119.123.58.104	DDoS
115.234.74.87	DDoS
58.62.164.163	DDoS
113.142.72.205	DDoS
36.102.236.6	DDoS
36.102.238.134	DDoS
60.164.222.77	DDoS
58.44.138.158	DDoS
114.244.117.216	DDoS
171.118.120.244	DDoS
185.234.219.106	Port Scan
162.243.128.21	Port Scan
192.241.238.242	Port Scan
192.241.237.157	Port Scan
162.243.128.228	Port Scan
192.241.237.108	Port Scan
162.243.128.195	Port Scan
192.241.202.110	Port Scan

37.49.226.10	Port Scan
128.199.85.18	Phishing
45.9.148.125	Malware
45.9.148.129	Malware
199.231.85.124	Malware
194.26.29.114	Phishing
173.82.168.10	Phishing
212.237.63.113	Port Scan
128.199.85.18	Port Scan
134.209.193.62	Port Scan
217.182.64.245	Port Scan
195.123.214.221	Phishing
157.245.239.186	Phishing
104.251.210.189	Phishing
104.206.225.254	Phishing
195.123.208.185	Phishing
167.172.145.74	Phishing
162.243.131.94	Port Scan
104.244.77.150	DDoS
192.241.235.214	Port Scan
45.13.93.82	Port Scan
3.132.217.43	Port Scan
50.7.146.43	Malware
193.56.28.177	Port Scan
193.56.28.193	Port Scan
199.127.61.237	Port Scan
23.228.67.70	Port Scan
192.241.238.14	Port Scan
95.168.171.154	Port Scan
162.243.131.54	Port Scan
5.196.198.39	Port Scan
162.243.131.201	Port Scan
162.243.133.226	Port Scan
51.89.234.101	Port Scan
167.172.132.243	DDoS
192.241.194.53	Port Scan
45.134.179.243	Port Scan
175.199.169.145	Port Scan
194.26.29.119	Port Scan
194.26.29.120	Port Scan
173.214.172.3	Port Scan

195.154.232.135	Port Scan
192.241.235.236	Port Scan
167.114.126.57	Phishing
212.237.63.113	Phishing
162.243.128.119	Port Scan
69.64.43.20	Port Scan
192.241.237.166	Port Scan
54.175.125.227	Port Scan
192.241.239.62	Port Scan
80.82.65.190	Port Scan
37.49.226.118	Port Scan
185.36.81.42	Port Scan
80.58.184.14	DDoS
182.139.137.201	Port Scan
162.243.129.231	Port Scan
128.199.194.77	Port Scan
162.243.128.16	Port Scan
144.208.127.93	Phishing
195.123.213.68	Phishing
191.241.238.239	Port Scan
103.145.13.9	Port Scan
162.243.130.88	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.

- Nicolle Bravo. Twitter: @NicolleABG
- Cristóbal Herrera. Linkedin: https://www.linkedin.com/in/cherrera0001/
- Nicolás Fernández. Linkedin: https://www.linkedin.com/in/nicolas-fernandez-6415b377/
- Claudio Pontigo. Linkedin: https://www.linkedin.com/in/clapontigo/

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: 2020.04.10 15:24:37 -04'00'