13BCS20-00053-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Cibernética

Publicado el Viernes 8 de Mayo de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 30 de Abril y el miércoles 06 de Mayo de 2020.

Falsificación de Registro o Identidad

8FFR20-00372-01 CSIRT ADVIERTE DE 3 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00372-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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 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/8ffr20-00372-01/

https://www.csirt.gob.cl/media/2020/04/8FFR20-00372-01.pdf

8FFR20-00373-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00373-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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/8ffr20-00373-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00373-01.pdf

8FFR20-00374-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00374-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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 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/8ffr20-00374-01/
https://www.csirt.gob.cl/media/2020/04/8FFR20-00374-01.pdf

8FFR20-00375-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00375-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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/8ffr20-00375-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00375-01.pdf

8FFR20-00376-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00376-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 de Abril de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco 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/8ffr20-00376-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00376-01.pdf

8FFR20-00377-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00377-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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 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/8ffr20-00377-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00377-01.pdf

8FFR20-00378-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00378-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo 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 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/8ffr20-00378-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00378-01.pdf

8FFR20-00379-01 CSIRT ADVIERTE DE 3 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00379-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo 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 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/8ffr20-00379-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00379-01.pdf

8FFR20-00380-01 CSIRT ADVIERTE ACTIVACIÓN DE DOS SITIOS PÚBLICOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00380-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo 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 Chile Atiende y Clave Única, 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/8ffr20-00380-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00380-01.pdf

8FFR20-00381-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00381-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento asociados a unaIP que suplanta el sitio web oficial de Banco 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/8ffr20-00381-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00381-01.pdf

8FFR20-00382-01 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00382-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo 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 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/8ffr20-00382-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00382-01.pdf

8FFR20-00383-01 CSIRT INFORMA DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00383-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Mayo de 2020
Última revisión	01 de Mayo 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/8ffr20-00383-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00383-01.pdf

8FFR20-00384-01 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00384-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Mayo de 2020
Última revisión	05 de Mayo 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/8ffr20-00384-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00384-01.pdf

8FFR20-00385-01 CSIRT HA IDENTIFICADO CUATRO PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00385-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a una IP que suplantan el sitio web oficial de Banco Estado , el que podría servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/alertas/8ffr20-00385-01/

https://www.csirt.gob.cl/media/2020/05/8FFR20-00385-01.pdf

8FFR20-00386-01 CSIRT ADVIERTE DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00386-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo 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/8ffr20-00386-01/

https://www.csirt.gob.cl/media/2020/05/8FFR-00386-01.pdf

8FFR20-00387-01 CSIRT ADVIERTE DE UN SITIO BANCARIO FRAUDULENTO

Alerta de seguridad cibernética	8FFR20-00387-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo 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 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/8ffr20-00387-01/

https://www.csirt.gob.cl/media/2020/05/8FFR20-00387-01.pdf

8FFR20-00388-01 CSIRT ADVIERTE DE SEIS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00388-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis 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/8ffr20-00388-01/

https://www.csirt.gob.cl/media/2020/05/8FFR20-00388-01.pdf

8FFR20-00389-01 CSIRT INFORMA DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad cibernética	8FFR20-00389-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo 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/8ffr20-00389-01/
https://www.csirt.gob.cl/media/2020/05/8FFR20-00389-01.pdf

Phishing

8FPH20-00201-01 CSIRT ADVIERTE DE PHISHING SOBRE FALSA PROMOCIÓN DE CERVEZA

Alerta de seguridad cibernética	8FPH20-00201-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 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 de la marca de cerveza Corona. El atacante busca que las personas utilicen un enlace adjunto.

El mensaje informa que cerveza Corona está regalando una hielera llena de cerveza. Para ello las personas deben responder una encuesta que les permitiría recibir el beneficio. Al terminar la encuesta aparece un supuesto proceso de verificación, donde se le solicita a la víctima compartir el mensaje de la promoción con al menos 15 contactos de WhatsApp. De esta manera el atacante expande su ataque abarcando más usuarios para ser afectados.

Al analizar las URLs del proceso de verificación asociados a la falsa promoción se identificó que redirigía a sitios de baja reputación y publicidad no deseada.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00201-01/
https://www.csirt.gob.cl/media/2020/04/8FPH20-00201-01.pdf

8FPH20-00202-01 CSIRT ADVIERTE PHIHSING POR SUSPENSIÓN DE SERVICIO EN CORREO CORPORATIVO

Alerta de seguridad cibernética	8FPH20-00202-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Mayo de 2020
Última revisión	04 de Mayo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de del correo electrónico supuestamente proveniente de Microsoft Outlook. El atacante intenta persuadir a la víctima para que utilice un enlace adjunto en el correo.

El mensaje informa que su cuenta de correo electrónico está a punto de ser suspendida. Para que esto no suceda, la persona debe verificar –se asume que se refiere a algún tipo de información que pues no se especifica- en un enlace que el atacante disponibiliza.

Si una persona selecciona el enlace, será es dirigida a un sitio falso del correo corporativo Outlook donde se le solicitará el nombre de usuario y contraseña y se expondrá a perder información sensible.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00202-01/

https://www.csirt.gob.cl/media/2020/05/8FPH20-00202-01.pdf

8FPH20-00203-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR BONO FAMILIAR COVID-19

Alerta de seguridad cibernética	8FPH20-00203-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Mayo de 2020
Última revisión	04 de Mayo 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. Los atacantes buscan que las personas utilicen un enlace en el cuerpo del correo.

El mensaje del correo informa a las personas que son beneficiarios del bono ayuda familiar Covid-19 que deben ingresar al enlace para revisar el depósito, ya que el IPS (Instituto de Previsión Social) instruyó depositarlos en las cuentas para evitar ir a una sucursal bancaria.

Si las personas seleccionan el enlace serán dirigidas a un sitio falso del banco, donde se exponen al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00203-01/

https://www.csirt.gob.cl/media/2020/05/8FPH20-00203-01.pdf

8FPH20-00204-01 CSIRT ADVIERTE DE PHISHING POR SATURACIÓN DE ALMACENAMIENTO EN CORREO

Alerta de seguridad cibernética	8FPH20-00204-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de del correo electrónico de un administrador de correo no identificado. El atacante busca persuadir al receptor para responder el mensaje enviado.

El mensaje informa a la víctima que el correo electrónico a superado el límite de almacenamiento definido por el administrador y no podrá recibir ni enviar correos. Para que esto no suceda, la persona debe verificar su cuenta enviando su nombre, el usuario, la contraseña, la casilla de correo electrónico y el email.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00204-01/
https://www.csirt.gob.cl/media/2020/05/8FPH20-00204-01.pdf

8FPH20-00205-01 CSIRT ADVIERTE PHISHING QUE INCENTIVA USO DE NUEVO PORTAL

Alerta de seguridad cibernética	8FPH20-00205-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo 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 intenta persuadir a la potencial víctima para utilizar un enlace en el cuerpo del correo.

El mensaje del correo informa e invita a utilizar el nuevo portal de auto atención digital, donde brindaran las respuestas a las dudas respecto al uso de tus productos financiaros.

El atacante disponibiliza un enlace para poder ingresar al nuevo portal. De seleccionarlo, la persona es dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00205-01/
https://www.csirt.gob.cl/media/2020/05/8FPH20-00205-01.pdf

8FPH20-00206-01 CSIRT ADVIERTE DE PHISHING POR DEPÓSITO DE PENSIONES

Alerta de seguridad cibernética	8FPH20-00206-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo 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 atacante busca persuadidor a quien recibe el mensaje de utilizar un enlace adjunto.

El mensaje del correo informa que por la contingencia de los últimos días, las pensiones o beneficios IPS de mayo ya se encuentran depositado a su Cuenta Rut para atender a sus necesidades financieras, e insiste en que no tiene que salir de casa para obtener el beneficio.

El atacante disponibiliza un enlace. Si la persona lo selecciona será dirigida a un sitio falso del banco, donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00206-01/
https://www.csirt.gob.cl/media/2020/05/8FPH20-00206-01.pdf

Vulnerabilidades

9VSA20-00196-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR ADOBE PARA ADOBE BRIDGE

Alerta de seguridad cibernética	9VSA20-00196-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 de Abril de 2020

Vulnerabilidad

CVE-2020-9553
CVE-2020-9554
CVE-2020-9555
CVE-2020-9556
CVE-2020-9557
CVE-2020-9558
CVE-2020-9559
CVE-2020-9560
CVE-2020-9561
CVE-2020-9562

CVE-2020-9563
CVE-2020-9564
CVE-2020-9565
CVE-2020-9566
CVE-2020-9567
CVE-2020-9568
CVE-2020-9569

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00196-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00196-01.pdf

9VSA20-00197-01 CSIRT COMPARTE ACTUALIZACIONES DE ADOBE PARA MAGENTO

Alerta de seguridad cibernética	9VSA20-00197-01
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-2020-9576,
CVE-2020-9577,
CVE-2020-9578,
CVE-2020-9579,
CVE-2020-9580,
CVE-2020-9581,
CVE-2020-9582,
CVE-2020-9583,
CVE-2020-9584,
CVE-2020-9585,
CVE-2020-9587,
CVE-2020-9588,
CVE-2020-9591

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00197-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00197-01.pdf

9VSA20-00198-01 CSIRT COMPARTE ACTUALIZACIONES DE APACHE PARA APACHE TRAFFIC SERVER

Alerta de seguridad cibernética	9VSA20-00198-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 de Abril de 2020

Vulnerabilidad

CVE-2020-9481

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00198-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00198-01.pdf

9VSA20-00199-01 CSIRT COMPARTE ACTUALIZACIONES DE JUNIPER PARA EL SO JUNOS

Alerta de seguridad cibernética	9VSA20-00199-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Abril de 2020
Última revisión	30 de Abril de 2020

Vulnerabilidad

CVE-2020-1631

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Juniper referente a vulnerabilidad que afecta al Sistema Operativo Junos. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00199-01/
https://www.csirt.gob.cl/media/2020/04/9VSA20-00199-01.pdf

9VSA20-00200-01 CSIRT COMPARTE ACTUALIZACIONES ENTREGADAS POR F5 PARA SUS PRODUCTOS

Alerta de seguridad cibernética	9VSA20-00200-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Mayo de 2020
Última revisión	02 de Mayo de 2020

Vulnerabilidad

CVE-2020-5880 CVE-2020-5893
CVE-2020-5889 CVE-2020-5890
CVE-2020-587 CVE-2020-5873
CVE-2020-5875 CVE-2020-5872
CVE-2020-5883 CVE-2020-5878
CVE-2020-5888 CVE-2020-5892
CVE-2020-5876 CVE-2020-5877
CVE-2020-5884 CVE-2020-5891
CVE-2020-5871 CVE-2020-5881
CVE-2020-5887 CVE-2020-5886
CVE-2020-5879 CVE-2020-5885

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por F5 referente a vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00200-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00200-01.pdf

9VSA20-00201-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR MOZILLA PARA FIREFOX IOS

Alerta de seguridad cibernética	9VSA20-00201-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Mayo de 2020
Última revisión	03 de Mayo de 2020

Vulnerabilidad

CVE-2020-6830

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00201-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00201-01.pdf

9VSA20-00202-01 CSIRT COMPARTE ACTUALIZACIONES DE OPENLDAP

Alerta de seguridad cibernética	9VSA20-00202-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Mayo de 2020
Última revisión	03 de Mayo de 2020

Vulnerabilidad

CVE-2020-12243

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00202-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00202-01.pdf

9VSA20-00203-01 CSIRT COMPARTE ACTUALIZACIONES DE GOOGLE PARA CHROME

Alerta de seguridad cibernética	9VSA20-00203-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Vulnerabilidad

CVE-2020-6464
CVE-2020-6831
CWE-119

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00203-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00203-01.pdf

9VSA20-00204-01 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA PARA FIREFOX Y FIREFOXESR

Alerta de seguridad cibernética	9VSA20-00204-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Vulnerabilidad

CVE-2020-6831
CVE-2020-12387
CVE-2020-12388
CVE-2020-12389
CVE-2020-12390
CVE-2020-12391
CVE-2020-12392
CVE-2020-12393
CVE-2020-12394
CVE-2020-12395
CVE-2020-12396

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Mozilla referente a múltiples vulnerabilidades que afectan a sus exploradores Firefox y Firefox ESR. El presente informe incluye la respectiva medida de mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00204-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00204-01.pdf

9VSA20-00205-01 CSIRT COMPARTE ACTUALIZACIONES PARA AVIRA

Alerta de seguridad cibernética	9VSA20-00205-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Vulnerabilidad

CVE-2020-12463

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00205-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00205-01.pdf

9VSA20-00206-01 CSIRT COMPARTE ACTUALIZACIONES LIBERADAS POR CITRIX

Alerta de seguridad cibernética	9VSA20-00206-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Mayo de 2020
Última revisión	06 de Mayo de 2020

Vulnerabilidad

CVE-2020-7473
CVE-2020-8982
CVE-2020-8983

Resumen

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

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00206-01/
https://www.csirt.gob.cl/media/2020/05/9VSA20-00206-01.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
162.243.144.29	Port Scan
162.243.138.213	Port Scan
162.243.137.24	Port Scan
54.38.248.131	Port Scan
162.243.142.15	Port Scan
162.243.138.114	Port Scan
162.243.143.93	Port Scan
5.189.131.63	Port Scan
51.15.165.218	Port Scan
45.125.66.21	Port Scan
102.129.224.174	Port Scan
162.243.135.248	Port Scan
162.243.136.142	Port Scan
162.243.138.70	Port Scan

162.243.137.42	Port Scan
162.243.144.176	Port Scan
162.243.145.60	Port Scan
162.243.144.248	Port Scan
157.230.126.210	Port Scan
162.243.141.212	Port Scan
162.243.139.32	Port Scan
162.243.141.51	Port Scan
162.243.137.88	Port Scan
162.243.143.92	Port Scan
162.243.144.103	Port Scan
162.243.139.83	Port Scan
37.49.226.166	Port Scan
45.95.168.212	Port Scan
162.243.144.239	Port Scan
162.243.135.192	Port Scan
162.243.144.211	Port Scan
162.243.139.225	Port Scan
162.243.143.7	Port Scan
162.243.138.139	Port Scan
162.243.136.110	Port Scan
162.243.141.142	Port Scan
162.243.138.186	Port Scan
45.67.14.21	Port Scan
162.243.139.197	Port Scan
162.243.139.141	Port Scan
162.243.137.241	Port Scan
162.243.145.81	Port Scan
144.91.127.239	Port Scan
89.248.168.218	Port Scan
195.231.1.46	Port Scan
73.142.15.62	Port Scan
104.153.105.179	Port Scan
162.243.142.164	Port Scan
162.243.136.115	Port Scan
162.243.143.115	Port Scan
62.243.144.173	Port Scan
162.243.143.30	Port Scan
162.243.139.184	Port Scan
162.243.142.72	Port Scan
162.243.136.60	Port Scan

162.243.141.131	Port Scan
162.243.144.213	Port Scan
162.243.138.64	Port Scan
162.243.143.206	Port Scan
162.243.138.26	Port Scan
162.243.144.4	Port Scan
156.96.114.98	Port Scan
162.243.141.165	Port Scan
162.243.140.177	Port Scan
162.243.145.52	Port Scan
162.243.135.161	Port Scan
162.243.139.205	Port Scan
162.243.144.156	Port Scan
162.243.141.77	Port Scan
157.245.48.44	Port Scan
162.243.138.127	Port Scan
162.243.139.93	Port Scan
92.118.234.186	Port Scan
102.129.224.252	Port Scan
162.243.138.132	Port Scan
185.232.65.24	Port Scan
45.143.220.93	Port Scan
172.107.225.206	Port Scan
199.195.254.100	Port Scan
198.148.27.38	Port Scan
193.227.234.37	Port Scan
193.227.234.34	Port Scan
193.227.234.35	Port Scan
193.227.234.38	Port Scan
193.227.234.36	Port Scan
162.243.138.207	Port Scan
205.185.124.190	Port Scan
51.159.55.71	Port Scan
196.201.35.219	Port Scan
196.201.35.222	Port Scan
162.243.135.56	Port Scan
51.79.21.228	Port Scan
162.243.139.70	Port Scan
45.143.221.50	Port Scan
167.114.125.234	Port Scan
161.129.70.74	Port Scan

139.99.137.224	Port Scan
45.14.151.246	Port Scan
94.102.50.155	Port Scan
1.32.250.67	Port Scan
72.12.194.91	Port Scan
72.12.194.94	Port Scan
72.12.194.92	Port Scan
72.12.194.90	Port Scan
72.12.194.93	Port Scan
162.243.136.230	Port Scan
162.243.144.229	Port Scan
162.243.144.7	Port Scan
162.243.144.212	Port Scan
162.243.145.59	Port Scan
162.243.143.205	Port Scan
162.243.140.88	Port Scan
162.243.138.125	Port Scan
165.227.210.114	Port Scan
162.243.137.45	Port Scan
162.243.137.242	Port Scan
162.243.137.123	Port Scan
162.243.144.151	Port Scan
162.243.145.44	Port Scan
162.243.142.126	Port Scan
162.243.138.85	Port Scan
162.243.143.230	Port Scan
162.243.136.42	Port Scan
162.243.144.139	Port Scan
162.243.137.157	Port Scan
162.243.136.27	Port Scan
162.243.144.63	Port Scan
162.243.144.76	Port Scan
142.77.2.85	Port Scan
66.216.18.222	Port Scan
198.82.247.34	Port Scan
172.104.212.253	Port Scan
142.93.212.109	Port Scan
162.243.145.45	Port Scan
176.107.131.129	Port Scan
165.227.221.225	Port Scan
162.243.138.15	Port Scan

163.243.140.157	Port Scan
216.98.9.226	Port Scan
162.243.137.66	Port Scan
199.19.225.176	Port Scan
89.34.27.242	Port Scan
37.49.226.164	Port Scan
45.143.220.131	Port Scan
128.14.140.30	Port Scan
162.243.137.159	Port Scan
37.49.230.241	Port Scan
202.152.1.89	Port Scan
162.243.142.131	Port Scan
91.194.84.74	Port Scan
95.217.22.83	Port Scan
176.107.131.9	Port Scan
121.254.234.224	Port Scan
162.243.136.246	Port Scan
162.243.144.39	Port Scan
93.186.197.181	Port Scan
95.168.171.144	Port Scan
91.194.84.109	Port Scan
193.228.91.106	Port Scan
163.172.82.79	Port Scan
93.186.202.6	Port Scan
51.159.6.236	Port Scan
91.194.84.6	Port Scan
162.243.138.145	Port Scan
162.243.139.160	Port Scan
162.243.145.42	Port Scan
162.243.138.170	Port Scan
162.243.138.77	Port Scan
162.243.142.140	Port Scan
162.243.139.142	Port Scan
162.243.138.178	Port Scan
162.243.136.203	Port Scan
162.243.142.133	Port Scan
162.243.136.158	Port Scan
162.243.139.140	Port Scan
142.93.187.179	Port Scan
162.243.139.16	Port Scan
162.243.138.4	Port Scan

162.243.138.215	Port Scan
162.243.143.39	Port Scan
162.243..144.235	Port Scan
162.243.143.114	Port Scan
162.243.136.141	Port Scan
162.243.136.61	Port Scan
193.39.15.131	Port Scan
162.243.141.134	Port Scan
162.243.143.209	Port Scan
162.243.137.23	Port Scan
217.61.121.181	Phishing
195.123.214.140	Phishing
134.209.168.128	Port Scan
167.99.78.224	Port Scan
162.243.144.149	Port Scan
70.32.0.55	Port Scan
104.244.78.213	Port Scan
134.209.63.140	Port Scan
45.79.34.252	Port Scan
95.216.232.99	Port Scan
74.207.233.118	Port Scan
156.96.150.252	Port Scan
74.91.117.65	Port Scan
23.247.114.194	Port Scan
198.74.54.142	Port Scan
103.79.141.171	Port Scan
139.99.179.188	Port Scan
157.119.250.11	Port Scan
62.171.178.119	Port Scan
59.125.98.49	Port Scan
206.189.65.107	Port Scan
167.71.71.79	Port Scan
162.243.144.73	Port Scan
162.243.139.4	Port Scan
202.181.25.11	Port Scan
178.62.113.55	Port Scan
134.209.164.184	Port Scan
162.243.137.148	Port Scan
162.243.137.224	Port Scan
162.243.137.43	Port Scan
162.243.139.167	Port Scan

162.243.138.42	Port Scan
45.143.223.164	Port Scan
102.129.224.190	Port Scan
142.93.211.252	Phishing
162.243.139.153	Port Scan
1103.145.12.72	Port Scan
1.255.226.82	Hacking
162.243.144.160	Port Scan
118.174.21.41	Hacking
102.129.224.133	Port Scan
103.89.177.140	Hacking
162.243.138.71	Port Scan
104.218.48.196	Port Scan
82.102.173.72	Port Scan
54.38.92.35	Port Scan
167.172.226.189	Port Scan
162.243.141.184	Port Scan
193.42.99.162	Port Scan
139.59.116.115	Port Scan
61.216.2.79	Port Scan
167.99.51.170	Port Scan
146.0.227.246	Port Scan
116.203.2.148	Port Scan
193.10.255.99	Port Scan
37.49.226.235	Port Scan
141.98.10.61	Port Scan
80.82.70.194	Port Scan
51.81.125.159	Port Scan
144.217.34.151	Port Scan
200.60.91.42	Port Scan
162.243.137.221	Port Scan
162.243.141.93	Port Scan
162.243.138.56	Port Scan
47.44.39.146	Port Scan
91.141.0.165	Port Scan
139.162.126.103	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 Machado Villegas. (Linkedin: https://www.linkedin.com/in/rodrigo-machado-villegas)

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: 2020.05.08 17:53:59 -04'00'