13BCS-00024-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 04 de Octubre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 19 y el miércoles 02 de Octubre.

Falsificación de Registro o Identidad

8FFR-00066-001 CSIRT HA IDENTIFICADO DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00066-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a IP's 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/8ffr-00066-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00066-001.pdf

8FFR-00067-001 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00067-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos sitios fraudulentos asociados a IP's que suplantan la web oficial de Banco ESTADO, lo que podría servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00067-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00067-001.pdf

8FFR-00068-001 CSIRT ADVIERTE DE NUEVOS SITIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00068-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

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/8ffr-00068-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00068-001.pdf

8FFR-00069-001 CSIRT ADVIERTO DE CINCO PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00069-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2019
Última revisión	24 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cinco portales fraudulentos asociados a 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/8ffr-00069-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00069-001.pdf

8FFR-00061-001 CSIRT ADVIERTE DE DOS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00061-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2019
Última revisión	16 de Septiembre de 2019

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 Estado, los que podrían servir para robar credenciales de usuarios de esa entidad.
Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00061-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00061-001.pdf

8FFR-00070-001 CSIRT ADVIERTE DE LA ACTIVACIÓN DE 4 PORTALES BANCARIOS FRUDULENTOS

Alerta de seguridad informática	8FFR-00070-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2019
Última revisión	25 de Septiembre de 2019

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/8ffr-00070-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00070-001.pdf

8FFR-00071-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00071-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Septiembre de 2019
Última revisión	25 de Septiembre de 2019

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/8ffr-00071-001/
https://www.csirt.gob.cl/media/2019/09/8FFR-00071-001.pdf

8FFR-00072-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00072-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2019
Última revisión	30 de Septiembre de 2019

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/8ffr-00072-001/

https://www.csirt.gob.cl/media/2019/09/8FFR-00072-001.pdf

8FFR-00073-001 CSIRT ADVIERTE DE LA ACTIVACIÓN DE 19 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00073-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2019
Última revisión	30 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 19 sitios fraudulentos asociados a una IP que suplanta el sitio web oficial del Banco de Chile, los que podrían servir para robar credenciales de usuarios de esa entidad.

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

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00073-001/

https://www.csirt.gob.cl/media/2019/10/8FFR-00073-001.pdf

8FFR-00074-001 CSIRT ADVIERTE ACTIVACIÓN DE PORTAL BANACARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00074-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2019
Última revisión	30 de Septiembre de 2019

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/8ffr-00074-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00074-001.pdf

8FFR-00075-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO ASOCIADO A IP QUE PODRÍA SERVIR PARA EL ROBO DE CREDENCIALES DE USUARIOS

Alerta de seguridad informática	8FFR-00075-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2019
Última revisión	02 de Octubre de 2019

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/8ffr-00075-001/
https://www.csirt.gob.cl/media/2019/10/8FFR-00075-001.pdf

2CMV-00032-001 CSIRT ADVIERTE DE ACTIVACIÓN DE CAMPAÑAS DE EMOTET

Alerta de seguridad informática	2CMV-00032-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), informa la activación de múltiples campañas de phishing con carga del malware Emotet, con documento tipo Word adjuntos. El fenómeno ha sido recogido por diversos medios informativos de seguridad a nivel mundial. CSIRT ha podido identificar campañas dirigidas especialmente a Chile dentro de este contexto. Este informe se estará ampliando en la medida que se puedan reunir mayor antecedentes. Las fuentes utilizadas en este informe son abiertas. CSIRT quiere llamar la atención a las instituciones públicas y privadas para que tomen las precauciones respectivas y estén alertas a los correos y descargas de archivos.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00032-001/
https://www.csirt.gob.cl/media/2019/09/2CMV-00032-001.pdf

2CMV-00033-001 CSIRT ADVIERTE DE PHISHING CON MALWARE EN CORREO QUE SUPLANTA A LA TESORERÍA GENERAL DE LA REPÚBLICA

Alerta de seguridad informática	2CMV-00033-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2019
Última revisión	01 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene de la Tesorería General de la Republica. Los delincuentes buscan engañar a los usuarios advirtiéndoles sobre una supuesta liquidación tributaria impaga. A la potencial víctima se le ofrece la posibilidad de descargar, desde un enlace, el informe generado por el Servicio de Impuesto Internos. Al seleccionar el Hipervínculo, la víctima es direccionada automáticamente hasta el archivo malicioso. Este archivo, al ser ejecutado genera un proceso de instalación. Luego de la instalación, se genera una conexión a internet descargando un supuesto documentos Word, pero en realidad es un archivo Zip que contiene tres archivos más. Se adjuntan los indicadores de compromisos.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00033-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00033-001.pdf

2CMV-00033-002 CSIRT ADVIERTE DE PHISHING CON MALWARE EN CORREO DE INTERPOL

Alerta de seguridad informática	2CMV-00033-002
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2019
Última revisión	01 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración Centro Nacional de Ciberseguridad de la Policía de Investigaciones de Chile, ha identificado nuevos indicadores de compromisos de la campaña de phishing con malware asociado informada recientemente en la alerta 2CMV-00033-001. La campaña es perpetrada a través de un correo electrónico que supuestamente proviene de INTERPOL, correo que supuestamente es enviado desde una casilla de correo electrónico de la Policía de Investigaciones de Chile. Los criminales buscan engañar a los usuarios advirtiéndoles que existe un proceso criminal a su nombre, ofreciendo la posibilidad de descargar la información sobre el caso en el enlace que acompaña el texto del correo. El archivo, al ser ejecutado, se instala y genera una conexión a internet descargando un supuesto documento Word, pero en realidad es un archivo Zip que contiene tres archivos más. Se adjuntan los indicadores de compromisos.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00033-002/
https://www.csirt.gob.cl/media/2019/10/2CMV-00033-002.pdf

2CMV-00034-001 CSIRT ADVIERTE DE PHISHING CON MALWARE ASOCIADO A EMOTET

Alerta de seguridad informática	2CMV-00034-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2019
Última revisión	02 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado a Emotet. Estos correos contienen documentos tipo Word adjuntos, donde el atacante intenta persuadir a las víctimas para que abran el documento. Dichos correos se han identificado en campañas dirigidas a Chile.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00034-001/
https://www.csirt.gob.cl/media/2019/10/2CMV-00034-001.pdf

Vulnerabilidades

9VSA-00051-001 CSIRT COMPARTE ACTUALIZACIONES DE HARBOR

Alerta de seguridad informática	9VSA-00051-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	20 de Septiembre de 2019
Última revisión	20 de Septiembre de 2019

Vulnerabilidad

CVE-2019-16097

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información difundida por PaloAlto acerca de una vulnerabilidad crítica en Harbor que permite escalar a cualquier usuario hasta los privilegios de administrador.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00051-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00051-001.pdf

9VSA-00052-001 CSIRT COMPARTE ACTUALIZACIONES DE VMWARE Y SUS PARCHES

Alerta de seguridad informática	9VSA-00052-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Septiembre de 2019
Última revisión	20 de Septiembre de 2019

Vulnerabilidad

CVE-2017-16544
CVE-2019-5531
CVE-2019-5532
CVE-2019-5534
CVE-2019-5527
CVE-2019-5535

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información acerca de 6 vulnerabilidades, 3 de ellas crítica, que afectan a VMWare, sus productos afectados y las mitigaciones correspondientes.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00052-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00052-001.pdf

9VSA-00053-001 CSIRT COMPARTE ACTUALIZACIÓN DE CHROME PARA WINDOWS, MAC Y LINUX

Alerta de seguridad informática	9VSA-00053-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	21 de Septiembre de 2019
Última revisión	21 de Septiembre de 2019

Vulnerabilidad

CVE-2019-13685 CVE-2019-13687
CVE-2019-13688 CVE-2019-13686

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la versión de Chrome 77.0.3865.90 liberada por Google para Windows, Mac y Linux. Esa versión aborda una vulnerabilidad que podría ser explotada por un atacante para tomar el control en un sistema afectado.

CSIRT hace un llamado para que los usuarios y administradores revisen su versión de Chrome y apliquen las actualizaciones necesarias.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00053-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00053-001.pdf

9VSA-00054-001 CSIRT COMPARTE ACTUALIZACIONES PARA INTERNET EXPLORER

Alerta de seguridad informática	9VSA-00054-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Septiembre de 2019
Última revisión	24 de Septiembre de 2019

Vulnerabilidad

CVE-2019-1367

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a una vulnerabilidad que afecta a Internet Explorer.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00054-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00054-001.pdf

9VSA-00055-001 CSIRT COMPARTE ACTUALIZACIONES PARA HARBOR

Alerta de seguridad informática	9VSA-00055-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2019
Última revisión	23 de Septiembre de 2019

Vulnerabilidad

CVE-2019-16097

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por VMWare referente a una vulnerabilidad de escalamiento de privilegios en Harbor.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00055-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00055-001.pdf

9VSA-00056-001 CSIRT COMPARTE INFORMACIÓN SOBRE VULNERABILIDADES Y PARCHES EN PRODUCTOS DE APPLE

Alerta de seguridad informática	9VSA-00056-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Septiembre de 2019
Última revisión	28 de Septiembre de 2019

Vulnerabilidad

CVE-2019-8779
CVE-2019-8641

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte la información entregada por Apple referente a vulnerabilidades que afectan a sus productos y sus respectivos parches

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00056-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00056-001.pdf

9VSA-00057-001 CSIRT COMPARTE ACTUALIZACIONES DE EXIM PARA LINUX

Alerta de seguridad informática	9VSA-00057-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2019
Última revisión	01 de Octubre de 2019

Vulnerabilidad

CVE-2019-16928

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida del sitio web de EXIM, referente a una vulnerabilidad detectada en el agente de transferencia de correos EXIM para Linux, junto a su respectiva actualización para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00057-001/
https://www.csirt.gob.cl/media/2019/10/9VSA-00057-001.pdf

9VSA-00058-001 CSIRT COMPARTE ACTUALIZACIONES PARA PRODUCTOS APPLE

Alerta de seguridad informática	9VSA-00058-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Octubre de 2019
Última revisión	01 de Octubre de 2019

Vulnerabilidad

CVE-2019-8654
CVE-2019-8704
CVE-2019-8721
CVE-2019-8722
CVE-2019-8723
CVE-2019-8724
CVE-2019-8725
CVE-2019-8738
CVE-2019-8739
CVE-2019-8775

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida del sitio web de Apple, referente a vulnerabilidades que afectan a sus productos y sus respectivos parches.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00058-001/
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00058-001/

Alertas de Phishing

8FPH-00063-001 CSIRT ADVIERTE DE PHISHING BANCARIO EXPONIENDO A LOS USUARIOS AL ROBO DE SUS CREDENCIALES

Alerta de seguridad informática	8FPH-00063-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Octubre de 2019
Última revisión	02 de Octubre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Chile. El correo indica que se ha detectado una operación no habitual. Los estafadores disponibilizan un enlace para cancelar la operación, incitando a sus víctimas a ingresar al él, exponiéndolos al robo de sus credenciales desde un sitio semejando al del Banco.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00063-001/
https://www.csirt.gob.cl/media/2019/10/8FPH-00063-001.pdf

Reportes

10CND-00018-001 Informe sobre actividad maliciosa Emotet en Chile

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), emite el presente informe sobre el fenómeno de Emotet, distribuido por campañas de phishing con archivos adjuntos Word maliciosos, y que tiene relación con la alerta publicada el 24 de septiembre pasado con el código 2CMV-00032-001.

La alerta informaba sobre la activación de múltiples campañas nivel mundial, así como campañas dirigidas a Chile.

Esta publicación proporciona detalle del método de infección y el comportamiento de las campañas que están dirigidas contra nuestro país. Además se comparten indicadores de compromisos y formas de prevenir ataques de ingeniería social que son utilizados por los atacantes.

Si bien las técnicas descubiertas por este CSIRT ya han sido documentadas anteriormente, el objetivo de este documento es ilustrar a los usuarios respecto a la frecuencia de ocurrencia de estos eventos y las precauciones que deben ser consideradas.

Enlace

https://www.csirt.gob.cl/reportes/10cnd-00018-001/
https://www.csirt.gob.cl/media/2019/09/10CND-00018-001.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante la pasada semana 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:

IP´s	Motivo
185.53.88.54	Scanning
167.86.114.134	Scanning
77.247.109.29	Scanning
159.203.193.246	Scanning
157.245.68.205	Scanning
157.245.68.199	Scanning
185.216.140.108	Scanning
77.111.247.68	Scanning
64.235.37.103	Scanning
179.43.149.11	Vulnerabilidad
190.196.60.169	Scanning
186.10.136.78	Scanning
147.135.26.91	Phishing
157.245.110.23	Phishing
195.22.28.198	Malware
209.99.40.221	Malware
185.182.57.79	Vulnerabilidad
94.177.243.17	Scanning
37.120.152.186	Scanning
185.244.25.133	Scanning
37.49.231.132	Scanning
192.64.86.92	Scanning
5.9.137.105	Scanning
213.152.173.133	Scanning
212.83.148.254	Scanning
159.203.201.237	Scanning
77.247.110.215	Scanning
185.53.88.81	Scanning
185.244.25.203	Attack
162.242.150.89	Phishing
23.253.58.227	Phishing
77.247.110.196	Scanning
185.22.67.108	Malware
45.89.175.106	Scanning

190.119.180.226	Malware
203.150.19.63	Malware
190.3.183.19	Malware
71.244.60.230	Malware
45.79.130.89	Scanning
172.105.6.186	Scanning
95.171.222.186	Scanning
61.135.169.125	Scanning
80.211.246.118	Scanning
77.247.110.113	Scanning
192.99.30.200	Scanning
125.64.94.211	Scanning
157.245.72.214	Vulnerabilidad
208.100.26.229	Scanning
185.200.118.76	Scanning
159.203.193.49	Scanning
185.53.88.79	Scanning
212.83.137.50	Scanning
62.173.139.164	Scanning
169.239.182.217	Scanning
179.32.19.219	Scanning
177.246.193.139	Scanning
31.172.240.91	Scanning
152.169.236.172	Scanning
201.212.57.109	Scanning
222.214.218.192	Scanning
87.230.19.21	Scanning
46.105.131.87	Scanning
182.176.106.43	Scanning
83.29.180.97	Malware
181.36.42.205	Malware
200.21.90.6	Malware
123.168.4.66	Malware
151.80.142.33	Malware
159.65.241.220	Malware
43.229.62.186	Malware
190.1.37.125	Malware
209.99.40.227	Malware
208.100.26.251	Malware
189.223.228.181	Malware
200.71.148.138	Malware
185.141.25.116	Malware

190.10.194.42	Malware
146.88.240.6	Port Scan
159.203.201.201	Port Scan
95.168.180.88	Port Scan
185.200.118.73	Port Scan
186.11.60.99	Hacking
42.231.162.201	Hacking
185.176.27.250	Hacking
145.239.215.136	Port Scan
37.49.224.137	Port Scan
89.19.29.189	Hacking
23.91.71.247	Hacking
52.86.23.155	Port Scan
185.200.118.74	Port Scan
45.55.184.238	Hacking
109.104.79.48	Port Scan
181.198.67.178	Port Scan
190.55.86.138	Port Scan
37.235.52.71	Port Scan
194.58.56.80	Malware
178.210.87.251	Hacking
69.167.138.35	Hacking
218.64.56.150	Port Scan
1.201.136.144	Hacking
77.247.109.31	Port Scan
161.117.89.74	Hacking
178.62.63.148	Hacking
165.22.188.224	Hacking
104.148.105.4	Hacking
222.92.200.50	Hacking
185.200.118.48	Port Scan
82.165.84.48	Hacking
159.203.197.146	Port Scan
80.211.254.237	Port Scan
187.199.158.226	Malware
186.0.95.172	Malware
139.5.237.27	Malware
170.84.133.72	Malware
190.117.206.153	Malware
194.58.56.103	Malware
117.187.30.118	Port Scan
194.50.163.106	Malware

41.57.104.182	Malware
217.61.61.187	Port Scan
77.247.110.223	Port Scan
159.203.201.116	Port Scan
193.56.28.144	Port Scan
69.162.110.226	Port Scan
193.56.28.44	Port Scan
77.247.110.217	Port Scan
159.203.201.47	Port Scan
51.79.129.211	Port Scan
185.200.118.69	Port Scan
185.244.25.106	Hacking
185.244.25.107	Hacking
102.165.49.69	Malware
107.167.93.197	Malware
119.154.134.211	Malware
119.154.209.175	Malware
119.154.220.96	Malware
119.157.163.145	Malware
119.157.229.245	Malware
139.28.36.212	Malware
176.107.177.54	Malware
176.107.177.77	Malware
178.238.228.113	Malware
178.238.235.143	Malware
182.181.239.4	Malware
185.157.79.115	Malware
185.161.209.183	Malware
185.161.210.111	Malware
192.3.157.104	Malware
193.111.155.137	Malware
193.164.131.58	Malware
193.37.152.28	Hacking
213.136.69.224	Hacking
213.136.73.122	Hacking
213.136.84.43	Hacking
213.136.87.122	Hacking
45.138.172.161	Hacking
45.92.156.76	Hacking
46.246.85.129	Hacking
51.254.228.144	Hacking
5.189.131.67	Hacking

5.189.137.8	Hacking
5.189.143.225	Hacking
5.189.145.248	Hacking
5.189.152.147	Hacking
5.189.167.220	Hacking
5.189.167.23	Hacking
5.189.167.65	Hacking
5.199.170.149	Hacking
62.4.23.46	Hacking
79.134.225.77	Hacking
79.143.181.21	Hacking
79.143.188.166	Hacking
80.241.221.109	Hacking
87.247.155.111	Hacking
88.150.227.71	Hacking
93.104.213.217	Hacking
185.10.68.88	Port Scan
185.244.25.106	Hacking
132.148.251.30	Hacking
185.200.118.51	Port Scan
163.172.8.223	Port Scan
192.144.130.54	Hacking
222.186.31.46	Port Scan
185.200.118.39	Port Scan
201.214.74.71	Malware
66.228.32.31	Malware
116.197.130.24	Hacking
45.227.255.149	Hacking
182.243.91.145	Hacking
103.118.222.54	Hacking
141.98.83.6	Hacking
176.121.14.191	Hacking
186.10.16.244	Malware
198.134.112.241	Malware
176.121.14.183	Port Scan
172.104.211.182	Port Scan

URL	Motivo
https[:]//www[.]bancostado-cl[.]com/imagenes/comun2009/en-linea-personas[.]php	Phishing
http[:]//99mesotheliomalawyers[.]com	Malware
http[:]//ad2[.]admart[.]tv	Malware
http[:]//applemedia1218[.]com	Malware
http[:]//attachment[.]biz	Malware
http[:]//avssync3357[.]com	Malware
http[:]//bargainhoundblog[.]com	Malware
http[:]//bbmdroid[.]com	Malware
http[:]//bbmsync2727[.]com/cu/seventh%20pay%20commission%20salary%20calculator[.]xls	Malware
http[:]//bhai123[.]no-ip[.]biz	Malware
http[:]//bhai1[.]ddns[.]net/	Malware
http[:]//bluesync2121[.]com	Malware
http[:]//BytesData[.]mssql[.]somee[.]com	Malware
http[:]//ceengrmes[.]attachment[.]biz/?att=1450603943	Malware
http[:]//comdtoscc[.]attachment[.]biz/?att=1451926252	Malware
http[:]//comdtoscc[.]attachment[.]biz/?att=1453788170	Malware
http[:]//dvdonlinestore[.]net	Malware
http[:]//eastmedia1221[.]com	Malware
http[:]//eastmedia2112[.]com	Malware
http[:]//eastmedia3347[.]co[.]cc	Malware
http[:]//eastmedia3347[.]com	Malware
http[:]//facemedia[.]co[.]cc	Malware
http[:]//fileshare[.]attachment[.]biz/?att=1455255900	Malware
http[:]//globedigitalmedia[.]com	Malware
http[:]//halwachi50[.]mymediapc[.]net	Malware
http[:]//intribune[.]blogspot[.]com	Malware
http[:]//jasoncarlosscot[.]dynu[.]net	Malware
http[:]//kssync3343[.]com	Malware
http[:]//kssync3347[.]co[.]cc	Malware
http[:]//kssync3347[.]com	Malware
http[:]//mahee[.]kssync3343[.]co[.]cc	Malware
http[:]//mundial2018[.]duckdns[.]org	Malware
http[:]//mustache-styles[.]com	Malware
http[:]//mvssync8767[.]com	Malware
http[:]//naddyto[.]warzonedns[.]com	Malware
http[:]//onlinestoreonsale[.]com	Malware
http[:]//pradahandbagsshoes[.]com	Malware
http[:]//rebrand[.]ly/purchaseorder54326	Malware
http[:]//sahirlodhi[.]com/usr/a	Malware
http[:]//student3347[.]mooo[.]com	Malware

http[:]//sudhir71nda[.]no-ip[.]org	Malware
http[:]//tslserv[.]duckdns[.]org	Malware
http[:]//vhideip[.]com	Malware
http[:]//winupdater2112[.]com	Malware
http[:]//winupdatess[.]no-ip[.]biz	Malware
http[:]//wisheshub[.]com	Malware
http[:]//www[.]allixanes[.]com/ez3/	Malware
http[:]//webgoreds[.]com/Activacion/cuenta-hvbv/	Phishing
https[:]//apositive[.]be/	Malware
http[:]//benelist[.]cz/result	Malware
http[:]//cibonline[.]org/	Malware
http[:]//bobbysinghwpg[.]com/k3v1t3v4	Malware
http[:]//kitchenandgifts[.]com/77g643	Malware
http[:]//turniejkrzyz[.]za[.]pl/	Malware
http[:]//1dnscontrol[.]com/&quot	Malware
http[:]//bisericaromaneasca[.]ro/amfcy	Malware
http[:]//cipemiliaromagna[.]cateterismo[.]it/jhYGUhjb6t	Malware
http[:]//demelkwegtuk[.]nl/ub4btafy96	Malware
http[:]//staffsolut[.]nichost[.]ru/grh5444tg?nLSzrogs=YKmnTyaWP	Malware
http[:]//jaysonmorrison[.]com/	Malware
hxxp[:]//www[.]averybit[.]com/wp-content/uploads/d4	Malware
hxxp[:]//www[.]bulbulstore[.]com/configweb/82oua00_nmnza-219207040/	Malware
hxxp[:]//www[.]costaging[.]com/staffheroes/ak9qqa045	Malware
hxxp[:]//www[.]demo[.]econzserver[.]com/blackhood/gkxo2I	Malware
hxxp[:]//www[.]dev[.]yashcodigital[.]com/cgi-bin/h11	Malware
hxxp[:]//www[.]devcorder[.]com/yberdigital-info/vs8yoml510	Malware
hxxp[:]//www[.]dimsum[.]xp-gamer[.]com/cgi-bin/nl72965	Malware
hxxp[:]//www[.]divakurutemizleme[.]com/wp-content/p4481	Malware
hxxp[:]//www[.]dtupl[.]com/wp-admin/g3ei2390	Malware
hxxp[:]//www[.]eastwoodoutdoor[.]com/cgi-bin/t3186	Malware
hxxp[:]//www[.]elisabietta[.]com/wp-content/44bj2z00	Malware
hxxp[:]//www[.]esoftlensmurah[.]com/wp-admin/x0300	Malware
hxxp[:]//www[.]every-day-sale[.]com/ab/1kxf6j325978	Malware
hxxp[:]//www[.]fashionupnext[.]com/wp-content/0j6w3at1	Malware
hxxp[:]//www[.]finalchace[.]com/wp-includes/nm86909	Malware
hxxp[:]//www[.]globercm[.]com/wp-content/u43zzh54	Malware
hxxp[:]//www[.]greenbeanph[.]com/cgi-bin/10zho5	Malware
hxxp[:]//www[.]guanchangwen[.]com/nofij3ksa/t6524	Malware
hxxp[:]//www[.]gzbfashion[.]com/wp-content/259	Malware
hxxp[:]//www[.]hepsihediyelik[.]net/wp-admin/7l8ob60	Malware
hxxp[:]//www[.]inquireexpert[.]com/css/enkw243373	Malware
hxxp[:]//www[.]martx[.]com/hotel-telephones/3juc78242	Malware

hxxp[:]//www[.]mosheperes[.]xyz/images/rbx31fh71	Malware
hxxp[:]//www[.]praguelofts[.]fantasy-web[.]net/wp-content/yho3521	Malware
hxxp[:]//www[.]purepropertiesobx[.]com/menusa/edt222	Malware
hxxp[:]//www[.]purl[.]org/dc/terms/xmlns:dcmitype	Malware
hxxp[:]//www[.]saeblaser[.]com/wp-admin/jx7w814	Malware
hxxp[:]//www[.]sidanah[.]com/wp-admin/6dtjzp2161	Malware
hxxp[:]//www[.]vivekanandadegreecollege[.]com/wp-includes/j63213	Malware
hxxp[:]//www[.]westburydentalcare[.]com/wp-content/tc3q3db789	Malware
hxxp[:]//www[.]zimahenergy[.]com/wp-content/azwk6	Malware
Spbvoditel[.]ru	Malware
coinhive[.]com	Malware
compraok[.]com[.]br	Malware
calcoastlogistics[.]com	Malware
asliaypak[.]com	Malware
www[.]dailydot[.]com	Malware
www[.]tmdmagento[.]com	Malware
https://inegocios[.]cl/offlce/cmd-login=e1cbb08316a704d8f3ba7f66dd385d49/?reff=MzA0NTU1NzIzODRjMTIxZTM3NWM3ZWEwN2FkNTQ3OGY=	Phishing
https://bancoestado-cl[.]imagenes-comun2008[.]com/	Phishing
http://bncoestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php	Phishing
http://ec2-34-204-203-242[.]compute-1[.]amazonaws[.]com/imagenes/comun2008/	Phishing
http://www[.]tokenschile[.]com/	Phishing
www[.]lbancodlechileportalloginl[.]origene[.]co[.]in	Phishing
http://footballtimes[.]info	Malware
http://vegetableportfolio[.]com	Malware
http://windowsearchcache[.]com	Malware
http://electricalweb[.]org	Malware
http://upnpdiscover[.]org	Malware
http://www[.]lazymmfi[.]org/hiradc/lib/www[.]bancoestado	Phishing
https://www[.]stuevesiegel[.]com/assets/fpc/Activacion[.]php[.]cl	Phishing
https://www[.]itau[.]cl-wps2[.]xyz/	Phishing
www[.]itau[.]cl-wps1[.]xyz	Phishing
www[.]tarjetacencosud[.]cl-web[.]xyz/	Phishing
http://andr0ip[.]site/grow/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
https://www[.]bencostado[.]xyz/imagenes/comun2009/en-linea-personas[.]php	Phishing
http://trav3lcoin[.]net/single/imagenes/comun2008/banca-en-linea-personas[.]html	Phishing
todaynwescorp[.]com	Malware
http://li3ancocredichille[.]com/chile-personal/ingreso[.]html	Phishing
http://]3ancoocredichile[.]com/chile-personal/ingreso[.]html	Phishing
http://il3ancocredlchile[.]com/chile-personal/ingreso[.]html	Phishing

http://www[.]wwv-l3ancacredichille-cl[.]htlps-wwv-cmr-cl[.]com/personas-cl/ingreso[.]html	Phishing
http://jeitacave[.]org/ps004[.]jpg	Malware
http://141[.]98[.]216[.]130/1505132[.]jpg	Malware
http://141[.]98[.]216[.]130/1603232[.]jpg	Malware
http://141[.]98[.]216[.]130/1808132[.]jpg	Malware
http://141[.]98[.]216[.]130/pe[.]jpg	Malware
http://nw[.]brownsine[.]com/	Malware
http://141[.]98[.]216[.]130/1505164[.]jpg	Malware
http://zopso[.]org/	Malware
http://141[.]98[.]216[.]130/1808164[.]jpg	Malware
http://141[.]98[.]216[.]130/1603264[.]jpg	Malware
http://danangluxury[.]com/wp-content/uploads/KTgQsblu/	Malware
http://gcesab[.]com/wp-includes/customize/zUfJervuM/	Malware
http://autorepuestosdml[.]com/wp-content/CiloXIptI/	Malware
http://covergt[.]com/wordpress/geh7l30-xq85i1-558/	Malware
http://zhaoyouxiu[.]com/wp-includes/vxqo-84953w-5062/	Malware
http://rockstareats[.]com/wp-content/themes/NUOAajdJ/	Malware
http://inwil[.]com/wp-content/oyFhKHoe	Malware
http://inesmanila[.]com/cgi-bin/otxpnmxm-3okvb2-29756/	Malware
http://dateandoando[.]com/wp-includes/y0mcdp2zyq_lx14j2wh2-0551284557/	Malware

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

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.

- Germán Fernández - https://www.linkedin.com/in/gfdez/
- Víctor Herrera - https://www.linkedin.com/in/victor-herrera/
- Milton Matamala - https://www.linkedin.com/in/miltonmatamala/
- Hugo Miranda - https://www.linkedin.com/in/hugo-miranda-vera-1a972149/
- Juan López - https://www.linkedin.com/in/jclopezc/
- Pablo Ramírez - https://www.linkedin.com/in/pramirezh/

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.04 16:48:29 -03'00'