Boletín de Ciberseguridad N°3 | CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Miércoles 03 de Julio del 2019

8FPH-00039-001 CAMPAÑA DE PHISHING A TRAVÉS DE UN CORREO ELECTRÓNICO QUE INTENTA ENGAÑAR A LOS USUARIOS DEL BANCO ESTADO

Características
Alerta de Seguridad Informática (8FPH-00039-001)
Nivel de Riesgo: Alto
Tipo: Phishing
Fecha de lanzamiento original: 25 de junio de 2019 | Última revisión 25 de Junio 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 que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco para que vuelvan a activar su cuenta, de lo contraria podría quedar bloqueada. Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00039-001.pdf

8FPH-00040-002 PHISHING A TRAVÉS DE UN CORREO ELECTRÓNICO QUE INTENTA ENGAÑAR A LOS USUARIOS DEL BANCO ESTADO

Características
Alerta de Seguridad Informática (8FPH-00040-001)
Nivel de Riesgo: Alto
Tipo: Phishing
Fecha de lanzamiento original: 26 de Junio de 2019 | Última revisión 26 de Junio 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 que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco indicándoles que por motivos de seguridad han bloqueado clave de acceso a la banca en línea y ofrece la necesidad de que vuelvan a verificar su cuenta, Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/06/8FPH-00040-001.pdf
https://www.csirt.gob.cl/media/2019/06/8FPH-00040-002.pdf (Actualización)

10OTI-00010-001 PROBLEMAS EN LAS TRANSMISIÓN DE DATOS EN PLATAFORMAS DE REDES SOCIALES

Características
Alerta de Seguridad Informática (10OTI-00010-001)
Nivel de Riesgo: Bajo
Tipo: Otros Incidentes
Fecha de lanzamiento original: 03 de Junio de 2019 | Última revisión 03 de Junio de 2019

Resumen
CSIRT libera comunicado advirtiendo sobre problemas de transmisión de datos presentado en diferentes redes sociales durante el día miércoles 3 de julio de 2019.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/10OTI-00010-001.pdf

2CMV-00012-001 A TRAVÉS DE CORREOS SE INTENTA ENGAÑAR A USUARIOS SOBRE COMPRAS PENDIENTES

Características
Alerta de Seguridad Informática (2CMV-00012-001)
Nivel de Riesgo: Alto
Tipo: Malware
Fecha de lanzamiento Original: 03 de Julio de 2019 | Última revisión 03 de Julio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de correos electrónicos que intentan engañar a los usuarios adjuntando documentos de compras pendientes, los que solicitan la descarga de un documento adjunto en formato Word bajo los nombres “Shipping doc.doc.rtf” y “Shipping doc.doc.rtf”, el que

se utiliza para explotar las vulnerabilidades CVE2018-0802 y CVE-2017-0199 de Office. Además, existe un script en los documentos que es ejecutado por PowerShell el que descarga y ejecuta archivos maliciosos. Al ser infectado, el equipo realiza comunicaciones al servidor de comando y control (C&C).

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/2CMV-00012-001.pdf

INFORME MENSUAL DE TICKETS DE GESTIÓN DEL CSIRT CORRESPONDIENTE AL MES DE JUNIO DE 2019

Características
Informe de Gestión Mensual
Fecha de lanzamiento Original: 02 de Junio de 2019 | Última revisión 02 de Junio de 2019
Emitido por: CSIRT de Gobierno

Resumen
El informe contiene un resumen de la totalidad de los tickets procesados en el mes de junio de 2019. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets, da cuenta del porcentaje de tickets cerrados con éxito en el curso del mes y la proporción de aquellos que quedan por terminar. Así mismo, se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.
El reporte mensual muestra el origen o procedencia de la información que procesa CSIRT y presenta en términos porcentuales. Adicionalmente, entrega un desagregado con el detalle que permite conocer la participación de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.
Finalmente presenta información proveniente de la plataforma MISP que contiene la cantidad de posibles IoC's que se hayan detectado.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/Informe-Mensual-de-Tickets-Ciberseguridad-Junio-2019-CSIRT-Gob-002.pdf