CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 18 de Julio del 2019

Resumen de Reportes, Alertas e Indicadores informadas por CSIRT entre el Jueves 11 y el Miércoles 17 de Julio.

9VSA-00018-001 CSIRT COMPARTE INFORME DE ACTUALIZACIONES EN PRODUCTOS CISCO

Características

Alerta de Seguridad Informática (9VSA-00018-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 11 de Julio de 2019 | Última revisión 11 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte el siguiente informe referente a una vulnerabilidad en los productos Cisco Adaptive Security Appliance Software (ASA) y Firepower Threat Defense (FTD), elaborado a partir de la información publicada por el proveedor.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00018-001.pdf

8FPH-00042-001 CSIRT ADVIERTE DE PHISHING BANCARIO CON NOTIFICACIÓN TELEFÓNICA

Características

Alerta de Seguridad Informática (8FPH-00042-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 12 de Julio de 2019 | Última revisión 12 de Julio 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 de Chile. El correo trata de persuadir a los clientes indicándoles que tiene un premio de $500.0000 mil pesos en su línea de crédito, para que lo gaste en lo que desee. Para reclamar el premio el usuario debe actualizar sus datos. Al hacerlo, también participará de un sorteo de 30 ipads mini y 20 televisores 4k. Se indica en el correo que los días 15 de cada mes será publicado el sorteo en el sitio web y además serán notificados vía telefónica. Una vez que el usuario supuestamente actualiza sus datos a través del enlace, es redirigido a un sitio semejante al de Banco Chile.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00042-001.pdf

8FPH-00043-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR MANTENIMIENTO DE CUENTA.

Características

Alerta de Seguridad Informática (8FPH-00043-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 12 de Julio de 2019 | Última revisión 12 de Julio 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 se realizó un mantenimiento en sus servicios y se encontró un error en su cuenta, motivo por el cual se procedió al bloqueo temporal de la cuenta. Los criminales tratan de persuadir al usuario de seleccionar el link adjunto para restablecer la cuenta y así obtener las credenciales de acceso. Al seleccionar el enlace se redirige a la víctima a un sitio semejante al de Banco Estado.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00043-001.pdf

2CMV-00018-001 CSIRT ADVIERTE DE PHISHING CON MALWARE EN CORREO DE COPIA DE FACTURA.

Características

Alerta de Seguridad Informática (2CMV-00018-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware
Fecha de lanzamiento original: 15 de Julio de 2019 | Última revisión 15 de Julio 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 donde los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de una copia de factura, de la empresa Hellmann Worldwide S.A.

Al seleccionar la imagen adjunta, se desencadena la descarga de archivos maliciosos que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00018-001.pdf

2CMV-00019-001 CSIRT ADVIERTE DE PHISHING CON MALWARE EN TRANSFERENCIA AL EXTERIOR AVALADO POR DOCUMENTO BANCARIO

Características

Alerta de Seguridad Informática (2CMV-00019-001)
Nivel de Riesgo: Alto
Tipo: Phishing - Malware
Fecha de lanzamiento original: 15 de Julio de 2019 | Última revisión 15 de Julio 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 donde los delincuentes buscan engañar a los usuarios insinuando en el título del correo que existe una transferencia al exterior y que el Banco BBVA Continental S:A ha enviado un documento donde puede confirmar la recepción del pago.

Al seleccionar el documento adjunto, se desencadena la descarga de archivos maliciosos que en realidad en un troyano tipo RAT que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante. Estos troyano tiene una arquitectura de cliente y servidor.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00019-001.pdf

2CMV-00020-001 CSIRT ADVIERTE DE MALWARE URSINF QUE ROBA CREDENCIALES BANCARIAS Y CUENTAS.

Características

Alerta de Seguridad Informática (2CMV-00020-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con el Malware Ursinf, un troyano que es conocido por el robo de credenciales bancarias y cuentas en línea.

A pesar que los correos electrónicos vienen en idioma italiano, se recomienda tener precaución. Los delincuentes buscan engañar indicando que existe una declaración que puede ser visualizado presionando el link adjunto. Cuando la persona hace clic en el hipervínculo es dirigido a una página web de Google Drive, que abre otra página falsa donde muestra un documento en formato PDF e incentiva a descargarlo. Al ser descargado se desencadena la infección ejecutando archivos Visual Basic.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00020-001.pdf

2CMV-00021-001 CSIRT ADVIERTE SOBRE PHIHSING SOBRE ENCOMIENDA

Características

Alerta de Seguridad Informática (2CMV-00021-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con Malware, indicando que existe una encomienda sellada que contiene un documento. Este correo intenta engañar a quienes lo reciben al señalar que proviene de la empresa DHL.

El atacante incita a las víctimas a descargar un documento que, supuestamente, es la declaración completa de la encomienda. El documento es un archivo ISO, el que al ser ejecutado desencadena la infección.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00021-001.pdf

8FPH-00044-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR ACTUALIZACIÓN DE SERVIDORES

Características

Alerta de Seguridad Informática (8FPH-00044-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio 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 se realizó un proceso de actualización en sus servidores, sin embargo su cuenta se encuentra bloqueada temporalmente y para restablecerla debe hacer clic en un enlace (imagen) para así activar su cuenta inmediatamente. El mensaje estable que solo se puede realizar este procedimiento con el hipervínculo señalado en el correo, de esta forma los criminales tratan de persuadir a al usuario a realizar clic en el hipervínculo de la imagen, solicitando las credenciales de acceso. Este enlace redirige a la víctima a un sitio falso semejante al de Banco Estado.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00044-001.pdf

8FPH-00045-001 CSIRT ADVIERTE DE PHISHING BANCARIO POR SUSPENSIÓN DE CUENTA CORRIENTE

Características

Alerta de Seguridad Informática (8FPH-00045-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio 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 BCI. El correo trata de persuadir a los clientes del Banco indicándoles que su cuenta se encuentra suspendida temporalmente, ya que su correo se encuentra registrado erróneamente, persuadiendo a los usuarios que deben normalizar la situación a través del enlace indicado en el correo, enlace que redirige a un sitio, supuestamente, del Banco BCI.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/8FPH-00045-001.pdf

9VSA-00019-001 CSIRT COMPARTE INFORME CON ACTUALIZACIONES DE ORACLE

Características
Alerta de Seguridad Informática (9VSA-00019-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática comparte una información publicada por Oracle referente a parches de actualización críticos para la mitigación de diversas vulnerabilidades que afectan a sus productos. Esta actualización de parches críticos contiene 319 nuevas correcciones de seguridad.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/9VSA-00019-001.pdf

9VSA-00020-001 CSIRT COMPARTE INFORME DE MICRSOSOFT SOBRE VULNERABILIDAD EN WINDOWS DEFENDER APPLICATION CONTROL

Características
Alerta de Seguridad Informática (9VSA-00020-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

Resumen
Esta vulnerabilidad podría permitir a un atacante omitir la característica de seguridad en Windows Defender Application Control aprovechando de eludir el modo de lenguaje restringido en PowerShell Core.
Para aprovechar la vulnerabilidad, un atacante primero deberá tener acceso de administrador a la máquina local donde PowerShell se está ejecutando en el modo de lenguaje restringido. Al hacer eso, un atacante podría aprovechar la depuración de scripts para abusar de los módulos firmados de una manera no intencionada.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/9VSA-00020-001.pdf

8FPH-00046-001CSIRT ADVIERTE DE PHISHING DE EMPRESA DE STREAMING

Características

Alerta de Seguridad Informática (8FPH-00046-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio 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 supuestamente proviene de la empresa de Straming Netflix. El correo trata de persuadir que debe actualizar sus datos para continuar con el servicio, ya que su cuenta se encuentra cancelada por existir un problema con el pago

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/8FPH-00046-001.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:

31.214.246.176	107.170.237.132	119.18.195.200	216.218.206.95
77.247.108.154	107.170.237.194	122.224.64.44	59.175.144.11
77.247.110.157	107.170.239.125	124.156.192.62	62.173.151.34
77.247.110.169	162.243.144.216	157.230.250.18	62.173.151.34
77.247.110.191	162.243.151.176	162.243.136.28	68.183.76.81
77.247.110.197	183.129.154.155	178.211.51.225	77.247.110.42
77.247.110.211	185.222.211.230	178.62.243.75	80.82.77.240
77.247.110.238	185.229.225.150	183.2.202.41	81.22.45.151
77.247.110.243	192.210.198.202	185.136.159.10	81.22.45.25
77.247.181.162	198.199.105.199	185.148.147.93	86.105.25.86
80.211.250.181	103.240.140.10	185.175.93.105	92.118.37.70
85.229.225.150	107.170.194.57	185.209.0.17	92.119.160.52
89.248.168.176	107.170.199.82	185.254.122.22	92.42.108.54
104.131.176.211	107.170.238.62	188.165.235.21	93.126.60.101
107.170.197.213	107.170.239.22	19185.53.88.17	
107.170.198.115	107.170.240.8	194.28.112.49	
107.170.203.160	107.170.250.62	208.67.222.222	

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

CONTACTOS

https://www.csirt.gob.cl

+ (562) 24863850

@CSIRTGOB

https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.18 13:02:20 -04'00'