13BCS-00016-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Miércoles 31 de Julio de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 25 y el miércoles 31 de julio.

Noticias

Publicado 25 julio, 2019

Nueva Variante de BitPaymer Encontrada en Chile Renombrada como DoppelPaymer

La compañía de Ciberseguridad CrowdStrike estimo que la variante de BitPaymer, hallada por el CSIRT de Gobierno de Chile, es en realidad un nuevo tipo de Ransomware.

Enlace:
https://www.csirt.gob.cl/noticias/nueva-variante-de-bitpaymer-encontrada-en-chile-renombrada-como-doppelpaymer/

Publicado 26 julio, 2019

Ataque de Ransomware deja a Residentes de Johannesburgo Sin Electricidad

La compañía responsable de abastecer de agua potable a la ciudad sudafricana de Johannesburgo, City Power, sufrió un ataque de ransomware que afectó a sus bases de datos, aplicaciones y red.

Enlace:
https://www.csirt.gob.cl/noticias/ataque-de-ransomware-deje-a-residentes-de-johanesburgo-sin-electricidad/

Publicado 29 julio, 2019

Declaran Emergencia de Ciberseguridad por Tres Ataques de Ransomware en Escuelas del Estado de Lousiana en Estados Unidos

Los ataques se produjeron en la madrugada del domingo y pusieron en alerta a todas las agencias locales y al FBI.

Enlace:
https://www.csirt.gob.cl/noticias/declaran-emergencia-de-ciberseguridad-por-tres-ataques-de-ransomware-en-escuelas-del-estado-de-lousiana-en-estados-unidos/

Alertas de Phishing

CSIRT ADVIERTE DE PHISHING POR AUMENTO DE CUPO EN TARJETA DE CRÉDITO

Alerta de seguridad informática	8FPH-00049-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Julio de 2019
Última revisión	24 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 Chile. El correo informa a las víctimas que deben revisar si tienen un aumento de cupo en su tarjeta y/o línea de crédito, la cual tiene una vigencia hasta el 31 de julio del 2019. Para verificar la vigencia de la supuesta oferta, se invita al usuario a seleccionar el enlace indicado en el correo, direccionando al afectado a un sitio semejante al del banco para que entregue sus credenciales bancarias.

Enlace

https://www.csirt.gob.cl/media/2019/07/8FPH-00049-001.pdf

CSIRT ADVIERTE DE PHISHING POR FIN DE MEMBRESÍA DE SERVICIO DE TECNOLOGÍA DE SOFTWARE Y HARDWARE

Alerta de seguridad informática	8FPH-00050-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2019
Última revisión	25 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), gracias a la colaboración de un usuario de redes sociales, han identificado una campaña de phishing a través de un correo electrónico que intenta engañar a los usuarios de Apple. El asunto del correo informa sobre el "límite de la cuenta", pero también apunta a un documento adjunto que informa sobre la intrusión en la cuenta del usuario –temas que no están vinculados- y por ende, la compañía solicita confirmar la identidad del afectado. El mensaje interno, por su parte, habla específicamente del vencimiento de la membresía del servicio y por eso se habría bloqueado la cuenta, por lo que solicita actualizar los datos a través del enlace que se ofrece en el correo, el cual redirecciona a la persona a un sitio semejante al de Apple, para que entregue sus credenciales.

Enlace

https://www.csirt.gob.cl/media/2019/07/8FPH-00050-001.pdf

CSIRT ADVIERTE DE PHISHING BANCARIO POR MANTENIMIENTO DE SERVICIOS

Alerta de seguridad informática	8FPH-00051-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2019
Última revisión	29 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 Estado. El correo informa a las víctimas que se realizó un mantenimiento en los servicios del banco y producto de ello, se encontró un error en la cuenta del usuario. Lo anterior obligó al bloqueó de la cuenta, y la única forma de activarla nuevamente es seleccionando el enlace indicado en el correo. De este modo, el atacante intenta convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco.

Enlace

https://www.csirt.gob.cl/media/2019/07/8FPH-00051-001.pdf

Alertas de Malware

CSIRT ADVIERTE DE MALWARE EN CORREO DE PROCESO CRIMINAL

Alerta de seguridad informática	2CMV-00023-001
Clase de alerta	Código Malicioso
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2019
Última revisión	25 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 que supuestamente proviene del Ministerio de Justicia y Derechos Humanos

Los delincuentes buscan engañar a los usuarios advirtiéndoles de la falsa apertura de un proceso criminal en su contra, teniendo un plazo de 48 horas para recurrir en su defensa. Para facilitar el trámite, se adjunta en el correo una copia del proceso, un archivo en formato ZIP que al ser ejecutado desencadena la infección del malware que tiene la capacidad de recopilar información sin el consentimiento del usuario, dejando además, puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Enlace

https://www.csirt.gob.cl/media/2019/07/2CMV-00023-001.pdf

Vulnerabilidades

9VSA-00024-001 CSIRT ADVIERTE DE VULNERABILIDAD EN PROTOCOLO NTP

Alerta de seguridad informática	9VSA-00024-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Julio de 2019
Última revisión	25 de Julio de 2019

Vulnerabilidad

CVE-2019-11331

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por la empresa F5 Network ha notificado una vulnerabilidad con clasificación alta que afecta al protocolo NTP (Network Tipe Protcol). Un atacante podría explotar la vulnerabilidad para acceder a recursos, modificar archivos o bien realizar ataques de denegación de servicio.

Enlace

https://www.csirt.gob.cl/media/2019/07/9VSA-00024-001.pdf

9VSA-00025-001 CSIRT COMPARTE INFORMACIÓN SOBRE VULNERABILIDAD EN VXWORKS DE WIND RIVER

Alerta de seguridad informática	9VSA-00025-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2019
Última revisión	29 de Julio de 2019

Vulnerabilidad

CVE-2019-12256
CVE-2019-12257
CVE-2019-12255
CVE-2019-12260
CVE-2019-12261
CVE-2019-12263
CVE-2019-12258
CVE-2019-12259
CVE-2019-12262
CVE-2019-12264
CVE-2019-12265

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte la información entregada por la empresa Wind River acerca de vulnerabilidades que afectan a su producto VxWorks

Enlace

https://www.csirt.gob.cl/media/2019/07/9VSA-00025-001.pdf

9VSA-00026-001 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIÓN EN OPENLDAP

Alerta de seguridad informática	9VSA-00026-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Julio de 2019
Última revisión	30 de Julio de 2019

Vulnerabilidad

CVE-2019-13057

CVE-2019-13565

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Ubuntu acerca de vulnerabilidades que afectan a OpenLDAP.

Enlace

https://www.csirt.gob.cl/media/2019/07/9VSA-00026-001.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:

37.49.230.21
51.89.17.237
213.59.4.26
77.247.110.210
77.247.110.212
77.247.110.209
151.15.103.53
63.143.52.74
77.247.110.111
81.22.45.18
81.22.45.19
81.22.45.250
81.22.45.253
68.210.78.84
218.92.1.141
198.108.67.48
107.170.204.13
77.247.108.159
119.147.213.222
141.98.80.115
112.85.42.176
103.31.54.69
119.18.195.196
103.31.54.67
107.170.196.235
216.245.210.54
107.170.201.70
222.85.25.115
176.107.130.153
104.244.72.28
77.247.110.236
185.232.67.121
185.53.88.132
178.211.51.222
185.236.76.216
194.254.212.30
185.70.184.32
31.133.49.60
42.231.162.192
86.104.72.51

2.114.244.170
103.117.172.206
103.117.232.198
103.207.1.44
103.84.238.3
107.172.143.241
107.173.42.177
125.99.253.34
131.0.142.120
131.196.184.141
131.255.82.24
138.121.24.78
144.217.12.34
146.196.122.152
146.196.122.167
162.247.155.131
164.132.138.134
168.227.229.112
168.235.102.16
177.103.240.149
177.52.79.29
177.8.172.86
180.250.197.188
181.115.168.69
181.129.140.140
181.129.49.98
181.129.93.226
185.180.197.38
185.202.174.72
185.251.38.35
186.183.199.114
186.42.186.202
186.42.226.46
187.58.56.26
189.80.134.122
190.152.4.210
190.154.203.218
191.37.181.152
192.227.232.26
192.243.101.232
195.123.246.69
202.4.169.178
23.94.93.106
36.89.85.103
45.237.240.178
5.253.63.112
51.254.69.233
103.231.146.242
151.61.68.155

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.31 18:37:00 -04'00'