Boletín de Ciberseguridad N°4 | CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Miércoles 10 de Julio del 2019

Resumen de Reportes, Alertas e Indicadores informadas por CSIRT entre el Jueves 4 y el Miércoles 10 de Julio.

2CMV-00013-001 URL QUE SIMULA PERTENECER A SITIO BANCARIO

Características

Alerta de Seguridad Informática (2CMV-00013-001)
Nivel de Riesgo: Alto
Tipo: Malware
Fecha de lanzamiento original: 05 de julio de 2019 | Última revisión 05 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una URL utilizada para engañar a los usuarios al simular un sitio de la banca. Esta dirección puede ser utilizada para ser insertada en correos electrónicos o archivos adjuntos para cometer fraudes. La URL indicada contiene un archivo ejecutable, que en realidad es un malware Troyano que rastrea los datos ingresados con el teclado, aplicaciones instaladas y realiza captura de pantallas, entre otras acciones. Además deja la posibilidad de insertar nuevos malware a través de la comunicación con el servidor comando control, para así aumentar su vector de ataque insertando nuevos módulos de malware en el equipo infectado.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00013-001-2.pdf

2CMV-00014-001 INFORME RANSOMWARE RYUK

Características

Alerta de Seguridad Informática (2CMV-00014-001)
Nivel de Riesgo: Alto
Tipo: Informe Ransomware Ryuk
Fecha de lanzamiento original: 05 de julio de 2019 | Última revisión 05 de Julio de 2019

Resumen

Ryuk fue descubierto en Agosto de 2018 y desde entonces ha sido responsable de múltiples ataques a nivel global. Ryuk es un Ransomware diseñado para realizar ataques dirigidos, los que realiza de cuerdo a la capacidad de pago de las víctimas. Ryuk es un Ransomware imperceptible después de la infección inicial. Los atacantes que utilizan Ryuk penetran en las redes a través de vulnerabilidades descubiertas y pueden pasar días o meses antes de propagarse, lo que permite al código malicioso reconocer la red infectada, identificando y apuntando a la red crítica del sistema, para así maximizar el impacto del ataque. Pero también ofrece el potencial de mitigar el ataque antes de que ocurra, si la infección inicial se detecta oportunamente y se logra remediar

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/2CMV-00014-001.pdf

8FPH-00041-001 PHISHING BANCARIO PIDE REINGRESAR DATOS EN WEB

Características

Alerta de Seguridad Informática (8FPH-00041-001)
Nivel de Riesgo: Alto
Tipo: Phishing
Fecha de lanzamiento original: 05 de Julio de 2019 | Última revisión 05 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 por motivos de seguridad han bloqueado la clave de acceso a la banca en línea y ofrece la posibilidad de verificar su cuenta ingresando al link indicado en el correo. Al seleccionar el enlace redirigen a la víctima a un sitio semejante al de Banco Estado, tratando de convencer a las personas para que ingresen sus credenciales de acceso y así obtener sus datos.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/8FPH-00041-001-1.pdf

2CMV-00015-001 CSIRT ADVIERTE SOBRE VARIAS CAMPAÑAS DE PHISHING CON EL ACTOR TA505

Características
Alerta de Seguridad Informática (2CMV-00015-001)
Nivel de Riesgo: Alto
Tipo: Malware Grupo TA505
Fecha de lanzamiento original: 05 de Julio de 2019 | Última revisión 05 de Julio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha observado varias campañas de phishing con el actor TA505 (nombre asignado por Proofpoint). Este grupo utiliza los troyanos bancarios Dridex y Locky ransomware y Rat. En los últimos análisis se ha observado en sus ataques otras familias de malware como FlawedGrace, FlawedAmmy y ServHelper. Según investigaciones de TredMicro estos ataques se han observado en los países como Emiratos Árabes Unidos, Arabia Saudita, India, Japón, Argentina, Filipinas y Corea del Sur. CSIRT también ha identificado campañas en Chile. Los atacantes utilizan como vector de entrada los correos electrónicos para poder infectar los equipos, el correo electrónico que contiene archivo adjunto como Word o Excel y URL'S maliciosas. Al ser ejecutado el documento, se instala automáticamente una función macro que ejecuta un proceso y, a su vez, descarga un archivo MSI, el cual ejecuta otro ejecutable en la memoria para luego tener comunicación con server comando control

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/2CMV-00015-001.pdf

2CMV-00016-001 NUEVA VARIANTE DE RANSOMWARE BITPAYMER

Características
Alerta de Seguridad Informática (2CMV-00016-001)
Nivel de Riesgo: Alto
Tipo: Informe de Ransomware
Fecha de lanzamiento original: 06 de Julio de 2019 | Última revisión 06 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha detectado muestras de Ransomware coincidentes con una nueva variante de BitPaymer, que afecta sistemas operativos de la familia Windows de Microsoft. Dentro de los efectos producidos por el Ransomware, están los de cifrar archivos de extensiones conocidas, modificándolas a ".locked", junto con la creación de un nuevo archivo el cual mantiene el nombre original seguido de la extensión txt.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/2CMV-00016-001.pdf

2CMV-00017-002 CSIRT ACTUALIZA INFORMACIÓN QUE ADVIERTE DE MALWARE EN CORREOS DE PHISHING DIRIGIDO A CONTRIBUYENTES DE IMPUESTOS

Características
Alerta de Seguridad Informática (2CMV-00017-001 y 2CMV-00017-002)
Nivel de Riesgo: Alto
Tipo: Phishing - Malware
Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 10 de Julio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración del Departamento TI del Servicio Nacional de Aduanas, ha identificado dos campañas de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Internos. Los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de un segundo aviso, lo que haría presumir al usuario que habría un correo anterior que no leyó, por lo que genera un incentivo para revisar el contenido de esta supuesta cadena de correos. El contenido del mensaje advierte a los usuarios que, para evitar una sanción económica que podría ascender a 100 UTM, deben descargar un supuesto documento de restitución de la declaración. El otro correo indica que el usuario tiene una deuda pendiente y debe descargar el detalle a través de un enlace. Al seleccionar dicho enlace, se desencadena la descarga de archivos maliciosos, que tienen 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.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/2CMV-00017-001.pdf
https://www.csirt.gob.cl/media/2019/07/2CMV-00017-002.pdf

9VSA-00013-001 CSIRT ADVIERTE SOBRE VULNERABILIDAD EN SOFTWARE DE VÍDEO CONFERENCIAS ZOOM

Características

Alerta de Seguridad Informática (9VSA-00013-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes Sobre Seguridad Informática, (CSIRT), advierte sobre el software de vídeo conferencias Zoom el cual presenta una vulnerabilidad que permitiría a un atacante tener acceso a la cámara del usuario sin previa autorización.
CVE-2019-13449: Una atacante remoto puede provocar una denegación de servicio utilizando una secuencia inválida hacia el cliente Zoom (versiones anteriores a 4.4.2 en macOS) CVE-2019-13450: En la aplicación Zoom Client y RingCentral para macOS, un atacante remoto puede obligar al usuario a unirse a un video llamado con la cámara activa. Esto ocurre porque cualquier sitio puede interactuar con el servidor web levantado localmente en los puertos 19421 y 19424. Nota: una máquina permanecerá vulnerable aun cuando el cliente haya sido desinstalado.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00013-001.pdf

9VSA-00014-001 CSIRT COMPARTE INFORME SOBRE LOS PARCHES PUBLICADOS POR MICROSOFT

Características

Alerta de Seguridad Informática (9VSA-00014-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, (CSIRT), comparte la información entregada hoy por Microsoft que lanzó un conjunto de actualizaciones de seguridad de software para el mes de julio para "parchear" un total de 77 vulnerabilidades, 14 de las cuales están clasificadas como críticas, 62 como importantes y una (1) está clasificada de gravedad moderada.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00014-001.pdf

9VSA-00015-001 CSIRT COMPARTE INFORME SOBRE VULNERABILIDAD PARCIAL SOBRE DENEGACIÓN DE SERVICIO EN ESXI

Características

Alerta de Seguridad Informática (9VSA-00015-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, (CSIRT), comparte información sobre una vulnerabilidad parcial publicada por VMware Security Response sobre denegación de servicio en ESXi. Los parches y soluciones están disponibles actualmente para remediar o solucionar esta vulnerabilidad.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00015-001.pdf

9VSA-00016-001 CSIRT COMPARTE INFORMACIÓN SOBRE ACTUALIZACIONES DE ADOBE

Características

Alerta de Seguridad Informática (9VSA-00016-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 10 de Julio de 2019 | Última revisión 10 de Julio de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, (CSIRT), comparte información sobre las actualizaciones de seguridad emitidas por Adobe para Adobe Bridge CC (APSB19-37), Experience Manager (APSB19-38) y Dreamweaver (APSB19-40). Los atacantes podrían explotar una de estas vulnerabilidades para tomar control de sistemas afectados.

Detalle disponible en el enlace:

https://www.csirt.gob.cl/media/2019/07/9VSA-00016-001.pdf

9VSA-00017-001 CSIRT COMPARTE ACTUALIZACIONES DE MOZILLA

Características
Alerta de Seguridad Informática (9VSA-00017-001)
Nivel de Riesgo: Alto
Tipo: Vulnerabilidad
Fecha de lanzamiento original: 10 de Julio de 2019 | Última revisión 10 de Julio de 2019

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática comparte el informe con las actualizaciones liberadas por Mozilla para el navegador Firefox que remedia distintas vulnerabilidades detectadas.

Detalle disponible en el enlace:
https://www.csirt.gob.cl/media/2019/07/9VSA-00017-001.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:

43.224.225.220	102.165.37.145	146.185.25.180
49.255.238.226	103.208.33.229	146.185.25.181
77.247.108.144	103.21.59.123	146.185.25.182
77.247.110.188	107.170.237.32	146.185.25.186
77.247.110.193	109.238.14.179	146.185.25.188
77.247.110.227	119.23.150.111	148.70.18.164
102.157.206.139	129.28.29.30	160.153.235.53
104.238.151.101	13.56.21.136	167.71.178.217
107.170.202.182	13.56.21.156	176.121.14.181
162.243.151.186	13.59.252.68	184.105.192.2
162.243.151.238	140.143.191.26	185.105.7.231
165.227.180.210	141.98.80.67	185.173.35.53
178.156.202.250	142.4.5.115	185.176.27.178
185.208.208.198	146.185.25.164	185.176.27.42
192.144.182.157	146.185.25.168	185.53.88.24
198.204.231.250	146.185.25.175	185.56.80.48
216.218.135.114	146.185.25.176	185.81.157.145
216.218.185.162	146.185.25.179	185.86.78.235

192.16.58.8	210.245.26.174	51.79.68.84
192.99.237.135	31.220.17.180	52.205.205.56
193.56.28.120	37.0.72.36	64.31.33.66
193.56.28.200	37.49.231.107	80.82.77.240
193.56.28.241	45.254.25.201	82.80.158.118
201.247.151.51	46.101.188.45	83.222.97.19
202.108.1.142	46.17.46.97	89.248.172.85
202.112.51.133	46.17.47.140	92.118.160.21
206.189.149.65	46.4.71.229	
208.91.107.66	51.68.192.110	

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: 2019.07.11 18:26:55 -04'00'