13BCS-00021-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Jueves 05 de Septiembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 29 y el miércoles 04 de Septiembre.

Noticias

Publicado 31 agosto, 2019

OEA destaca aporte del marco de ciberseguridad en infraestructuras críticas del Instituto de Estándares y Tecnologías (NIST) de los EE.UU

El documento califica al marco NIST como una herramienta de gestión de riesgos que habilita la innovación tecnológica y capaz de ajustarse a cualquier tipo de organización. Bajo esta perspectiva, el marco NIST podría servir como referencia para el futuro modelo de gobernanza en ciberseguridad chileno.

Enlace:
https://www.csirt.gob.cl/noticias/oea-destaca-aporte-del-marco-de-ciberseguridad-en-infraestructuras-criticas-del-instituto-de-estandares-y-tecnologias-nist-de-los-ee-uu/

Publicado 01 septiembre, 2019

Chile formaliza creación del CSIRT de Gobierno

La Resolución Exenta 5.006 formaliza al Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) como un Departamento dentro de la estructura del gobierno, específicamente en la Subsecretaría del Interior y Seguridad Pública.

Enlace:
https://www.csirt.gob.cl/noticias/chile-formaliza-creacion-del-csirt-de-gobierno/

8FFR-00034-001 CSIRT ADVIERTE DE UN NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00034-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Agosto de 2019
Última revisión	31 de Agosto de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portal fraudulentos asociados a una IP que suplantan el sitio web oficial del **bancoestado.cl**, 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/media/2019/08/8FFR-00034-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00034-001/

8FFR-00035-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00035-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portal fraudulentos asociados a una IP que suplantan el sitio web oficial del **bancoestado.cl**, 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/media/2019/09/8FFR-00035-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00035-001-csirt-advierte-de-sitio-bancario-fraudulento/

8FFR-00036-001 CSIRT ADVIERTE SOBRE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00036-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 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 del **bancochile.cl**, 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/media/2019/09/8FFR-00036-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00036-001/

8FFR-00037-001 CSIRT ADVIERTE DE NUEVO PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00037-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancochile.cl, 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/media/2019/09/8FFR-00037-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00037-001/

8FFR-00038-001 CSIRT advierte de activación de sitio bancario FRAUDULENTO

Alerta de seguridad informática	8FFR-00038-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancofalabella.cl, 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/media/2019/09/8FFR-00038-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00038-001-csirt/

8FFR-00039-001 CSIRT INFORMA DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00039-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoScotiaBank.cl, 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/media/2019/09/8FFR-00039-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00039-001/

8FFR-00040-001 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00040-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoSantander.cl, 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/media/2019/09/8FFR-00040-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00040-001/

8FFR-00041-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00041-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoItau.cl, 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/media/2019/09/8FFR-00041-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00041-001/

8FFR-00042-001 CSIRT INFORMA DE LA ACTIVACIÓN DE UN PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00042-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoBCI.cl, 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/media/2019/09/8FFR-00042-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00042-001/

8FFR-00043-001 CSIRT ADVIERTE DE PORTAL FRAUDULENTO BANCARIO

Alerta de seguridad informática	8FFR-00043-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoEstado.cl, 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/media/2019/09/8FFR-00043-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00043-001/

8FFR-00044-001 CSIRT INFORMA DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00044-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Septiembre de 2019
Última revisión	04 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 del bancoChile.cl, 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/media/2019/09/8FFR-00044-001.pdf
https://www.csirt.gob.cl/alertas/8ffr-00044-001/

Alertas de Phishing

8FPH-00058-001 CSIRT ADVIERTE DE PHISHING BANCARIO SOBRE MANTENIMIENTO DE SERVICIOS

Alerta de seguridad informática	8FPH-00058-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre 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 persuadir a los usuarios del Banco Estado, notificándoles en el correo que se realizó un mantenimiento en sus servicios. Debido a esta mantención, los criminales advierten a la potencial víctima sobre la detección de un error en su cuenta, y que por ese motivo se procedió al bloqueo de la misma. Para terminar de persuadir a la víctima, los estafadores señalan que la única forma de desbloquear la cuenta es ingresando al enlace que aparece en el correo. El atacante incita a sus víctimas para ingresar al enlace, exponiendo a los usuarios el robo de sus credenciales desde un sitio semejando al del Banco.

Enlace

https://www.csirt.gob.cl/media/2019/09/8FPH-00058-001.pdf
https://www.csirt.gob.cl/alertas/8fph-00058-001/

2CMV-00028-001 CSIRT ADVIERTE DE MALWARE ASOCIADO A CORREO DE PHISHING PROVENIENTE SUPUESTAMENTE DEL SII

Alerta de seguridad informática	2CMV-00026-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre 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 Servicio de Impuesto Interno. Los delincuentes buscan engañar a los usuarios advirtiéndoles sobre la existencia de una factura electrónica por la cual es necesario seleccionar el hipervínculo indicado en el correo. Para dar la impresión de legitimidad del remitente, el correo informa que las transacciones efectuadas entre los contribuyentes y su sitio web viajan de forma segura y confidencial, ya que el sistema de impuestos internos tiene implementado el sistema SSL. Toda la información que entrega el atacante intenta confundir al usuario para ganar su confianza y así, convencerlo para que descargué los archivos que permiten ejecutar y desencadenar a infección de malware.

Enlace

https://www.csirt.gob.cl/media/2019/09/2CMV-00028-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00028-001/

2CMV-00029-001 CSIRT ADVIERTE DE CAMPAÑA DE PHISHING CON MALWARE DESDE UN CORREO FALSO DE LA TESORERÍA GENERAL

Alerta de seguridad informática	2CMV-00029-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre 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 el hipervínculo indicado el informe generado por el Servicio de Impuesto Internos. Al descargar el archivo y ser ejecutado, desencadena la infección de malware.

Enlace

https://www.csirt.gob.cl/media/2019/09/2CMV-00029-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00029-001/

2CMV-00030-001 CSIRT ADVIERTE DE CAMPAÑA DE ADWARE

Alerta de seguridad informática	2CMV-00030-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado sitios relacionados con anuncios publicitarios no deseados (Adware). Este ataque de ingeniería social intenta persuadir a los usuarios para que seleccionen "permitir" en el mensaje que aparece en el navegador, lo que, como consecuencia, multiplicará el envío de anuncios no deseados directamente al equipo del afectado.

El anuncio puede ser activado al ingresar en algún sitio no confiable. El usuario será bombardeado de mensajes para ver contenidos o para descargar información.

También cabe la posibilidad que un usuario haya instalado algún software gratuito que contenga un Adware, por ejemplo, a través de una "Play Store" con aplicaciones (APK), ofreciendo anuncios no deseados. Dichas aplicaciones se hacen pasa por aplicaciones legítimas especialmente centrada en juegos y fotografías.

Enlace

https://www.csirt.gob.cl/media/2019/09/2CMV-00030-001.pdf
https://www.csirt.gob.cl/alertas/2cmv-00030-001-csirt-advierte-de-campana-de-adware/

Vulnerabilidades

9VSA-00040-001 CSIRT INFORMA DE VULNERABILIDAD DE LA PLATAFORMA STEAM

Alerta de seguridad informática	9VSA-00040-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de agosto de 2019
Última revisión	30 de agosto de 2019

Vulnerabilidad

CVE-2019-13516

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información recopilada desde diferentes fuentes referente a una vulnerabilidad detectada en el cliente STEAM de VALVE, y las respectivas recomendaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00040-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00040-001/

9VSA-00041-001 CSIRT INFORMA SOBRE VULNERABILIDADES EN PRODUCTOS CISCO

Alerta de seguridad informática	9VSA-00041-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de agosto de 2019
Última revisión	30 de agosto de 2019

Vulnerabilidad

CVE-2019-1977 CVE-2019-1964
CVE-2019-1968 CVE-2019-1965
CVE-2019-1967 CVE-2019-1966
CVE-2019-1969 CVE-2019-12643
CVE-2019-1963 CVE-2019-1944
CVE-2019-1962 CVE-2019-1945

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por CISCO referente vulnerabilidades detectadas en varios de sus productos y sus respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/08/9VSA-00041-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00041-001/

9VSA-00042-001 CSIRT COMPARTE INFORMACIÓN DE VULNERABILIDADES DE DEBIAN

Alerta de seguridad informática	9VSA-00042-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Septiembre de 2019
Última revisión	02 de Septiembre de 2019

Vulnerabilidad

CVE-2019-9517 CVE-2019-10092
CVE-2019-10081 CVE-2019-10097
CVE-2019-10082 CVE-2019-10098

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por DEBIAN referente vulnerabilidades detectadas en varios productos del servicio Apache2 httpd y sus respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/media/2019/09/9VSA-00042-001.pdf
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00042-001/

9VSA-00043-001 CSIRT COMPARTE ACTUALIZACIONES PARA FIREFOX ESR

Alerta de seguridad informática	9VSA-00043-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Septiembre de 2019
Última revisión	03 de Septiembre de 2019

Vulnerabilidad

CVE-2019-11746 CVE-2019-11752
CVE-2019-11744 CVE-2019-9812
CVE-2019-11742 CVE-2019-11743
CVE-2019-11753 CVE-2019-11740

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por MOZILLA referente vulnerabilidades detectadas en Firefox ESR, explorador para navegación en internet, junto con sus respectivas actualizaciones para mitigar el riesgo.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00043-001/
https://www.csirt.gob.cl/media/2019/09/9VSA-00043-001.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	Causa Asociada
109[.]94[.]209[.]91	Port Scan
139[.]180[.]195[.]36	Port Scan
159[.]69[.]54[.]146	Port Scan
185[.]142[.]98[.]41	Port Scan
185[.]17[.]122[.]220	Port Scan
185[.]225[.]17[.]5	Port Scan
195[.]123[.]213[.]126	Port Scan
160[.]119[.]253[.]219	Port Scan
169[.]239[.]128[.]29	Port Scan
169[.]239[.]128[.]36	Port Scan
45[.]84[.]0[.]82	Port Scan

119[.]18[.]195[.]194	Port Scan
185[.]53[.]88[.]41	Phishing
80[.]211[.]249[.]70	Phishing
77[.]247[.]110[.]83	Phishing
45[.]125[.]66[.]68	Phishing
209[.]239[.]112[.]150	Port Scan
62[.]210[.]89[.]217	Hacking
138[.]68[.]216[.]51	Port Scan
185[.]200[.]118[.]80	Hacking
208[.]91[.]112[.]55	DDoS
193[.]161[.]193[.]99	Port Scan
205[.]144[.]171[.]185	Port Scan
77[.]247[.]110[.]127	Port Scan
168[.]196[.]201[.]103	Malware
193[.]23[.]244[.]244	Malware
89[.]36[.]212[.]80	Hacking
42[.]231[.]162[.]203	Hacking
69[.]175[.]31[.]212	Hacking
185[.]244[.]31[.]29	Malware
23[.]227[.]207[.]157	Malware
41[.]203[.]73[.]126	Malware
23[.]226[.]131[.]150	Malware
194[.]5[.]98[.]24	Malware
5[.]187[.]34[.]115	Malware
139[.]162[.]28[.]163	Port Scan
198[.]98[.]62[.]183	Port Scan
77[.]247[.]108[.]202	Port Scan
167[.]71[.]253[.]81	Port Scan
212[.]83[.]158[.]206	Hacking
77[.]247[.]110[.]153	Port Scan
37[.]49[.]227[.]202	Hacking
3[.]87[.]11[.]10	Port Scan
37[.]49[.]231[.]121	Port Scan
192[.]254[.]185[.]30	Phishing
77[.]247[.]110[.]216	Hacking
81[.]22[.]45[.]225	Port Scan
185[.]156[.]177[.]248	Port Scan
138[.]68[.]216[.]227	Port Scan
138[.]68[.]212[.]170	Port Scan
138[.]68[.]216[.]217	Port Scan
138[.]68[.]212[.]207	Port Scan
185[.]175[.]93[.]18	Hacking

194[.]32[.]71[.]4	Hacking
185[.]222[.]211[.]114	Hacking
217[.]61[.]20[.]238	Hacking
185[.]200[.]118[.]47	Hacking
35[.]194[.]52[.]235	Hacking
89[.]38[.]145[.]124	Hacking
185[.]175[.]93[.]45	Hacking
185[.]175[.]93[.]21	Hacking
178[.]73[.]215[.]171	Hacking
14[.]225[.]3[.]37	Hacking
138[.]68[.]216[.]225	Port Scan
89[.]248[.]174[.]219	Port Scan
185[.]175[.]93[.]105	Port Scan
64[.]31[.]33[.]70	Port Scan
185[.]175[.]93[.]19	Port Scan
80[.]82[.]64[.]127	Port Scan
89[.]248[.]174[.]201	Port Scan
94[.]102[.]56[.]181	Port Scan
89[.]248[.]162[.]168	Port Scan
80[.]82[.]70[.]239	Port Scan
89[.]248[.]172[.]85	Port Scan
89[.]248[.]168[.]202	Port Scan
89[.]248[.]160[.]193	Port Scan
208[.]100[.]26[.]241	Port Scan
139[.]178[.]72[.]146	Port Scan
198[.]54[.]116[.]43	Port Scan
200[.]119[.]45[.]140	Port Scan
107[.]181[.]175[.]122	Port Scan
79[.]143[.]31[.]94	Port Scan
186[.]47[.]40[.]234	Port Scan
181[.]129[.]93[.]226	Port Scan
190[.]152[.]4[.]210	Port Scan

URL's Bloqueadas	Causas Asociadas
www[.]banco-estado[.]site	Phishing
http:[//]estado-personas[.]online/login/comun2019/banca-en-linea-personas[.]html	Phishing
c0n730[.]com/ALFALOAD-090319/index[.]php	Phishing
104[.]223[.]98[.]130/fourthenmay/iqXXCFVvD9a5J7H76KKFB8EDD00M86L989603G	Phishing
newage[.]radnewage[.]com	Malware
superalpha[.]radnewage[.]com	Malware
newghoul2019[.]radnewage[.]com	Malware
minernewage[.]com	Malware
newage[.]minernewage[.]com	Malware
mdwnte[.]com	Malware
rad2016[.]publicvm[.]com	Malware
hellothere[.]publicvm[.]com	Malware
radjoker2[.]publicvm[.]com	Malware
noobminer[.]publicvm[.]com	Malware
radpal[.]publicvm[.]com	Malware
newalpha[.]super-gamezer[.]com	Malware
roro2016[.]linkpc[.]net	Malware
newalpha[.]alphanoob[.]com	Malware
newblackage[.]com	Malware
noobminer[.]newblackage[.]com	Malware
newminersage[.]com	Malware
newminer[.]newminersage[.]com	Malware
newage[.]newminersage[.]com	Malware
superuser[.]newminersage[.]com	Malware
superlover[.]newminersage[.]com	Malware
blackjoker[.]newminersage[.]com	Malware
superalpha[.]newminersage[.]com	Malware
newghoul2019[.]newminersage[.]com	Malware
radnewage[.]com	Malware
suzano[.]sp[.]gov[.]br	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.

- Milton Matamala - https://www.linkedin.com/in/miltonmatamala/
- Juan Daniel Tolosa - https://www.linkedin.com/in/jdtolosa/

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.09.05
19:00:42 -04'00'