CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 06 de Febrero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 30 de Enero y el miércoles 04 de Febrero de 2020.

Falsificación de Registro o Identidad

8FFR20-00199-01 CSIRT ADVIERTE DE 11 SITIOS BANCARIOS FRUADULENTOS

Alerta de seguridad informática	8FFR20-00199-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Enero de 2020
Última revisión	30 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 11 portales fraudulentos asociado a una IP que suplantan diferentes sitios web oficiales de los bancos Estado, Security, de Chile, BCI, Scotiabank, Falabella, Santander, BICE, ITAU y Ripley. Estos portales podrían servir para robar credenciales de usuarios de esas entidades.

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/alertas/8ffr20-00199-01/

https://www.csirt.gob.cl/media/2020/01/8FFR20-00199-01.pdf

8FFR20-00200-01 CSIRT ADVIERTE DE CUATRO PORTALES BANCARIOS FRUADULENTOS

Alerta de seguridad informática	8FFR20-00200-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Enero de 2020
Última revisión	30 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial de Banco Estado, 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/alertas/8ffr20-00200-01/
https://www.csirt.gob.cl/media/2020/01/8FFR20-00200-01.pdf

8FFR20-00201-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00201-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Febrero de 2020
Última revisión	01 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a dos IP que suplantan el sitio web oficial de Banco Estado, 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/alertas/8ffr20-00201-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00201-01.pdf

8FFR20-00202-01 CSIRT ADVIERTE DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00202-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Febrero de 2020
Última revisión	01 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplanta el sitio web oficial de Banco Scotiabank, 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/alertas/8ffr20-00202-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00202-01.pdf

8FFR20-00203-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00203-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero de 2020

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 de Banco Falabella, 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/alertas/8ffr20-00203-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00203-01.pdf

8FFR20-00204-01 CSIRT ADVIERTE DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00204-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero de 2020

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 de Banco Estado, 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/alertas/8ffr20-00204-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00204-01.pdf

8FFR20-00205-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00205-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero de 2020

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 de Banco BCI, 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/alertas/8ffr20-00205-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00205-01.pdf

8FFR20-00206-01 CSIRT ALERTA DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00206-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de febrero de 2020
Última revisión	04 de febrero de 2020

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 de Banco Scotiabank, 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/alertas/8ffr20-00206-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00206-01.pdf

Malware

2CMV20-00046-01 CSIRT ADVIERTE DE MALWARE POR LIQUIDACIÓN TRIBUTARIA IMPAGA

Alerta de seguridad informática	2CMV20-00046-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware a través de un correo electrónico que utiliza el nombre de la Tesorería General de la República.

El mensaje del correo indica que existen obligaciones producto de una liquidación tributaria que se encuentra impaga.

En el mensaje se agrega un enlace a través del cual se descarga un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado, se realiza un proceso falso de instalación, pero en realidad se gatilla un script que descarga el malware.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00046-01/
https://www.csirt.gob.cl/media/2020/02/2CMV20-00046-01.pdf

2CMV20-00047-01 ADVIERTE DE MALWARE A TRAVÉS DE CORREO QUE INVITA A REUNIÓN

Alerta de seguridad informática	2CMV20-00047-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware que cita a la víctima a una reunión de trabajo. El mensaje del correo indica que se debe asistir a una reunión con urgencia, incluyendo un archivo ".doc", el cual, al momento de abrirlo, ejecuta un programa que instala el malware Emotet infectando a la víctima.

Enlace:

https://www.csirt.gob.cl/alertas/2cmv20-00047-01/
https://www.csirt.gob.cl/media/2020/02/2CMV20-00047-01.pdf

Phishing

8FPH20-00103-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR SUSPENSIÓN DE CUENTA

Alerta de seguridad informática	8FPH20-00103-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de un registro incorrecto de la cuenta. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que es necesario que ingrese para reactivar la cuenta o de lo contrario se procederá al bloqueo de los servicios por internet. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00103-01/
https://www.csirt.gob.cl/media/2020/01/8FPH20-00103-01.pdf

8FPH20-00104-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING EN SERVICIO STREAMING

Alerta de seguridad informática	8FPH20-00104-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios de la empresa de Streaming Netflix.

El correo indica que existe un problema con el monto de pago y solicita, a quien lo recibe, que normalice la situación lo antes posible para evitar problemas e interrupciones en el servicio. El atacante disponibiliza un enlace, que al ser seleccionado, redirige al usuario a un sitio semejante al de Netflix. En el sitio se solicita del usuario su nombre, número de tarjeta de crédito, fecha de caducidad y código de seguridad.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00104-01/

https://www.csirt.gob.cl/media/2020/01/8FPH20-00104-01.pdf

8FPH20-00105-01 CSIRT ADVIERTE PHISHING BANCARIO POR VERIFICACIÓN DE IDENTIDAD

Alerta de seguridad informática	8FPH20-00105-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de un error por la falta de verificación de identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que es necesario que ingrese para reactivar su cuenta. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00105-01/

https://www.csirt.gob.cl/media/2020/01/8FPH20-00105-01.pdf

8FPH20-00106-01 CSIRT ADVIERTE DE PHISHING BANCARIO POR RETENCIÓN DE FONDOS

Alerta de seguridad informática	8FPH20-00106-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de Febrero de 2020
Última revisión	1 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico dirigido a clientes del Banco Scotiabank.

En el mensaje los atacantes informan a la víctima sobre una supuesta transferencia de fondos retenida, acción que fue tomada por la propia seguridad del cliente. El phishing trata de persuadir a los usuarios para que revisan su estado de cuenta, lo que pueden realizar accediendo a un hipervínculo ubicado en el cuerpo del correo. Al seleccionar el enlace, el usuario es derivado a un sitio semejante al del banco.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00106-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00106-01.pdf

8FPH20-00107-01 ADVIERTE DE PHISHING BANCARIO POR RETENCIÓN DE FONDOS

Alerta de seguridad informática	8FPH20-00107-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Febrero de 2020
Última revisión	03 de Febrero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Scotiabank.

El mensaje informa a la víctima sobre la retención de una transferencia de fondos. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que es necesario que ingrese para revisar su estado de cuenta. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00107-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00107-01.pdf

9VSA20-00131-01 CSIRT COMPARTE ACTUALIZACIONES DE ADOBE PARA MAGENTO

Alerta de seguridad informática	9VSA20-00131-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Febrero de 2020
Última revisión	01 de Febrero de 2020

Vulnerabilidad

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Adobe referente a 6 vulnerabilidades que afectan a Magento Commerce y Open Source, 3 de ellas han sido clasificadas como críticas y 3 como importantes.

Resumen

CVE-2020-3715
CVE-2020-3718
CVE-2020-3716
CVE-2020-3719
CVE-2020-3717
CVE-2020-3758

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00131-01/
https://www.csirt.gob.cl/media/2020/01/9VSA20-00131-01.pdf

9VSA20-00132-01 CSIRT COMPARTE ACTUALIZACIONES DE DJANGO PARA SU WEB FRAMEWORK

Alerta de seguridad informática	9VSA20-00132-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de febrero de 2020
Última revisión	04 de febrero de 2020

Vulnerabilidad

CVE-2020-7471

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Django, referente a una vulnerabilidad que afecta a ambiente de desarrollo web, la cual de ser explotada permitiría a un atacante realizar inyecciones SQL permitiéndole obtener completo control sobre la aplicación y su base de datos. Este informe incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00132-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00132-01.pdf

Indicadores de Compromisos

Se comparte a continuación el listado de indicadores de compromisos que fueron detectados durante las pasadas dos semanas 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:

IoC	Motivo
149.56.242.200	Port Scan
151.106.10.17	Port Scan
37.49.230.90	Port Scan
68.183.29.48	Port Scan
45.143.220.120	Port Scan
142.93.212.170	Phishing
165.22.212.160	Phishing
216.245.218.178	Port Scan
149.56.28.5	Port Scan
139.99.39.31	Port Scan
217.61.20.142	Port Scan
107.175.89.162	Port Scan
103.76.22.118	Port Scan
5.135.253.172	Port Scan
109.236.109.159	Malware
85.96.49.152	Malware
186.10.98.177	Malware
45.55.65.92	Port Scan
67.227.152.142	Port Scan
147.91.209.151	Port Scan
37.1.201.184	Port Scan
185.53.88.123	Port Scan
167.99.96.138	Port Scan
190.186.164.23	Malware
2.45.112.134	Malware
31.16.195.72	Malware
191.103.76.34	Malware
93.144.226.57	Malware
168.126.149.11	Port Scan
35.246.66.189	Port Scan
220.128.159.121	Port Scan
172.245.24.138	Port Scan

201.47.196.59	Port Scan
51.254.23.227	Port Scan
178.32.126.225	Port Scan
185.222.66.98	Port Scan
58.182.154.127	Port Scan
90.140.136.100	Port Scan
128.199.81.66	Port Scan
89.163.225.107	Port Scan
86.62.195.78	Port Scan
51.89.99.60	Port Scan
95.234.58.254	Port Scan
192.95.13.168	Port Scan
158.69.120.179	Port Scan
165.227.16.98	Phishing
42.112.158.168	Port Scan
109.205.46.197	Port Scan
109.205.46.198	Port Scan
109.205.46.199	Port Scan
109.205.46.200	Port Scan
216.245.208.126	Port Scan
51.159.35.142	Port Scan
83.143.245.130	Port Scan
45.143.221.42	Port Scan
89.248.174.253	Port Scan
107.180.29.18	Phishing
92.119.121.230	Port Scan
162.243.128.149	Port Scan
192.241.232.150	Port Scan
103.108.7.226	Port Scan
162.243.129.77	Port Scan
194.26.29.129	Port Scan
45.14.224.2	Port Scan
164.160.21.203	Port Scan
188.24.28.2	Port Scan
116.88.64.32	Port Scan
206.219.100.104	Port Scan
94.102.51.22	Port Scan
162.243.128.103	Port Scan
162.243.130.155	Port Scan
189.90.202.214	Port Scan
192.241.231.223	Port Scan

192.241.229.150	Port Scan
162.243.131.166	Port Scan
162.243.131.157	Port Scan
162.243.128.230	Port Scan
162.243.130.225	Port Scan
162.243.128.186	Port Scan
192.241.233.177	Port Scan
162.243.130.49	Port Scan
45.148.10.89	Port Scan
162.243.128.91	Port Scan
162.243.128.183	Port Scan
162.243.131.90	Port Scan
192.241.239.84	Port Scan
104.206.128.2	Port Scan
162.243.129.98	Port Scan
162.243.128.45	Port Scan
162.243.128.252	Port Scan
211.110.211.6	Port Scan
192.241.237.202	Port Scan
192.241.222.59	Port Scan
192.241.239.124	Port Scan
162.243.131.194	Port Scan
185.53.88.91	Port Scan
5.66.42.153	Port Scan
192.241.238.132	Port Scan
162.243.131.125	Port Scan
162.243.130.31	Port Scan
162.243.131.80	Port Scan
162.243.130.126	Port Scan
162.243.129.67	Port Scan
162.243.130.16	Port Scan
192.241.238.142	Port Scan
192.241.239.229	Port Scan
183.129.18.106	DDoS
122.227.119.122	DDoS
60.176.209.123	DDoS
122.227.119.10	DDoS
115.217.183.90	DDoS
123.96.208.39	DDoS
92.246.76.253	Port Scan
97.104.251.173	Port Scan

167.99.151.177	Port Scan
192.241.236.64	Port Scan
162.243.131.118	Port Scan
162.243.130.48	Port Scan
162.243.129.223	Port Scan
192.241.239.138	Port Scan
51.15.209.167	Port Scan
51.158.96.215	Port Scan
163.172.132.238	Port Scan
192.241.239.119	Port Scan
192.241.233.240	Port Scan
192.241.230.235	Port Scan
162.243.130.173	Port Scan
162.243.128.127	Port Scan
162.243.129.241	Port Scan
162.243.131.101	Port Scan
69.113.200.154	Port Scan
162.243.130.70	Port Scan
162.243.129.115	Port Scan
92.246.84.195	Port Scan
162.243.130.140	Port Scan
162.243.129.30	Port Scan
45.143.223.156	Port Scan
99.190.197.63	Port Scan
162.243.130.188	Port Scan
162.243.131.107	Port Scan
192.241.231.5	Port Scan
162.243.131.84	Port Scan
162.243.128.188	Port Scan
192.241.238.218	Port Scan
162.243.130.203	Port Scan
58.182.136.252	Port Scan
192.241.238.92	Port Scan
162.243.131.38	Port Scan
216.170.125.195	Port Scan
192.241.235.209	Port Scan
192.241.228.216	Port Scan
162.243.131.38	Port Scan
201.33.175.1	Port Scan
192.241.239.29	Port Scan
192.241.210.47	Port Scan

192.241.239.30	Port Scan
192.241.239.112	Port Scan
192.241.239.88	Port Scan
192.241.239.78	Port Scan
92.63.194.104	Port Scan
192.241.210.68	Port Scan
162.243.130.131	Port Scan
162.243.129.121	Port Scan
162.243.130.226	Port Scan
172.58.172.207	Port Scan
162.243.128.158	Port Scan
163.47.57.41	Port Scan
172.58.172.222	Port Scan
51.89.125.114	Port Scan
162.243.131.129	Port Scan
156.238.190.230	Port Scan
174.236.2.115	Port Scan
192.241.192.208	Port Scan
162.243.129.113	Port Scan
162.243.128.227	Port Scan
162.243.131.55	Port Scan
162.243.130.135	Port Scan
162.243.129.41	Port Scan
162.243.129.48	Port Scan
59.92.71.71	Port Scan
162.243.129.106	Port Scan
192.241.239.139	Port Scan
162.243.128.12	Port Scan
162.243.131.136	Port Scan
192.241.234.94	Port Scan
192.241.238.144	Port Scan
192.241.238.241	Port Scan
162.243.131.74	Port Scan
198.199.94.90	Port Scan
192.241.238.131	Port Scan
80.211.10.42	Port Scan
62.171.135.227	Port Scan
162.243.128.49	Port Scan
162.243.129.167	Port Scan
192.241.226.184	Port Scan
163.172.198.253	Port Scan

162.243.131.64	Port Scan
192.241.237.105	Port Scan
192.241.238.119	Port Scan
46.38.144.109	Port Scan
46.38.144.142	Port Scan
192.241.211.169	Port Scan
42.115.22.145	Malware
118.98.75.85	Malware
107.181.187.155	Malware
41.185.66.173	Malware
89.252.141.160	Malware
145.14.144.154	Malware
43.255.154.93	Malware
45.55.179.121	Malware
162.243.131.31	Port Scan
162.243.129.21	Port Scan
162.243.131.58	Port Scan
41.227.51.40	Port Scan
45.143.221.40	Port Scan
192.241.232.70	Port Scan
216.245.196.222	Port Scan
162.243.130.210	Port Scan
162.243.129.33	Port Scan
162.243.130.93	Port Scan
162.243.128.13	Port Scan
162.243.128.199	Port Scan
5.12.103.35	Port Scan
27.125.183.38	Port Scan
58.96.235.109	Port Scan
58.96.236.128	Port Scan
79.113.125.153	Port Scan
82.76.214.160	Port Scan
86.107.75.122	Port Scan
94.102.49.102	Port Scan
103.95.1.53	Port Scan
162.243.128.160	Port Scan
162.243.129.20	Port Scan
162.143.130.25	Port Scan
162.243.130.119	Port Scan
183.90.110.246	Port Scan
192.241.233.61	Port Scan

192.241.238.124	Port Scan
192.241.238.207	Port Scan
192.241.239.135	Port Scan
198.199.119.181	Port Scan
222.164.156.148	Port Scan
192.241.239.66	Port Scan
185.89.102.53	Port Scan
185.89.102.57	Port Scan
185.89.102.47	Port Scan
208.73.211.165	Port Scan
203.196.19.22	Port Scan
148.72.232.65	Port Scan
88.42.32.78	Port Scan
2.32.49.227	Port Scan
88.57.72.14	Port Scan
194.243.5.17	Port Scan
195.103.133.46	Port Scan
151.75.115.83	Port Scan
2.247.254.232	Port Scan

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.

- Jair Palma Vincenty - https://www.linkedin.com/in/jair-palma-vicenty-62038920/
- Luis Miguel Ancapichun - https://www.linkedin.com/in/luis-miguel-ancapichun-b03a50159/

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: 2020.02.07 12:12:37 -03'00'