13BCS20-00044-01

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 06 de Marzo de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 27 de Febrero y el miércoles 04 de Marzo de 2020.

Falsificación de Registro o Identidad

8FFR20-00230-01 CSIRT ADVIERTE 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00230-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Febrero de 2020
Última revisión	27 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 tres IP que suplantan el sitio web oficial del 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/8ffr20-00230-01/

https://www.csirt.gob.cl/media/2020/02/8FFR20-00230-01.pdf

8FFR20-00231-01 CSIRT ADVIERTE DE 2 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00231-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Febrero de 2020
Última revisión	27 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 del 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/8ffr20-00231-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00231-01.pdf

8FFR20-00232-01 CSIRT ADVIERTE DE 3 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00232-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 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 del 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/8ffr20-00232-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00232-01.pdf

8FFR20-00233-01 CSIRT INFORMA DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00233-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 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 del 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/8ffr20-00233-01
https://www.csirt.gob.cl/media/2020/02/8FFR20-00233-01.pdf

8FFR20-00234-01 CSIRT ADVIERTE 2 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00234-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Febrero de 2020
Última revisión	29 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 dos IP que suplantan el sitio web oficial del 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/8ffr20-00234-01/
https://www.csirt.gob.cl/media/2020/02/8FFR20-00234-01.pdf

8FFR20-00235-01 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR20-00235-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Marzo de 2020
Última revisión	02 de Marzo 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 del 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/8ffr20-00235-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00235-01.pdf

8FFR20-00236-01 CSIRT IDENTIFICÓ 6 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00236-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Marzo de 2020
Última revisión	03 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de seis portales fraudulentos asociados a tres 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/8ffr20-00236-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00236-01.pdf

8FFR20-00237-01 CSIRT ADVIERTE DE 2 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00237-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Marzo de 2020
Última revisión	03 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IP que suplantan el sitio web oficial del 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/8ffr20-00237-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00237-01.pdf

8FFR20-00238-01 CSIRT INFORMA DE 2 PÁGINAS BANCARIAS FRAUDULENTAS

Alerta de seguridad informática	8FFR20-00238-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Marzo de 2020
Última revisión	03 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a cuatro IP que suplantan el sitio web oficial del 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/8ffr20-00238-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00238-01.pdf

8FFR20-00239-01 CSIRT ADVIERTE DE 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00239-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Marzo de 2020
Última revisión	04 de Marzo de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del 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/8ffr20-00239-01/
https://www.csirt.gob.cl/media/2020/03/8FFR20-00239-01.pdf

Phishing

8FPH20-00121-01 CSIRT ADVIERTE PHISHING DE UNA SUPUESTA OFERTA BANCARIA

Alerta de seguridad informática	8FPH20-00121-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 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 Estado.

El mensaje informa que el Banco refinanciará tus deudas, que existe un crédito pre aprobado y además podrá efectuar un avance de dinero con abono inmediato en tu cuenta, esta oferta tiene como vigencia hasta hoy 28 de febrero de 2020. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo. Al seleccionar el vínculo es dirigida a un sitio semejante al del banco donde se expone al robo de sus credenciales.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00121-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00121-01.pdf

8FPH20-00122-01 CSIRT ADVIERTE DE PHISHING BANCARIO DE ROBO DE CREDENCIALES

Alerta de seguridad informática	8FPH20-00122-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Febrero de 2020
Última revisión	29 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 atacante envía mensaje de diversos contenidos, por ejemplo:

- Existe una operación irregular y que debe verificar
- Que la cuenta se encuentra suspendida por no realizar el pago de los impuestos
- Que se ha bloqueado su cuenta por realizar una operación sospechosa
- Se ha suspendido por no pago de impuestos

De esa forma intenta persuadir al usuario que seleccione el enlace, al hacerlo, 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/8fph20-00122-01/
https://www.csirt.gob.cl/media/2020/02/8FPH20-00122-01.pdf

8FPH20-00123-01 CSIRT IDENTIFICÓ PHISHING DE SUPUESTAS ANOMALÍAS EN LA CUENTA BANCARIA

Alerta de seguridad informática	8FPH20-00123-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Marzo de 2020
Última revisión	01 de Marzo de 2020

Resumen

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

El mensaje informa a la víctima sobre la retención de una transferencia, producto de anomalías en la cuenta. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que la transferencia quedará retenida y será necesario acudir a una sucursal para el desbloqueo de la 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/8fph20-00123-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00123-01.pdf

8FPH20-00124-01 CSIRT ADVIERTE PHISHING BANCARIO POR VERIFICACIÓN DE IDENTIDAD

Alerta de seguridad informática	8FPH20-00124-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Marzo de 2020
Última revisión	04 de Marzo 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 que su cuenta se encuentra suspendida, arrojando un mensaje de "Error" en los sistemas del banco. El supuesto error se debe a que el usuario no habría realizado un procedimiento de verificación de identidad, el que necesariamente debe ser a través del sitio web. Bajo ese argumento, el atacante intenta persuadir a la víctima de acceder a un enlace que se adjunta en el cuerpo del correo, de lo contrario, la persona tendría que acercarse a una sucursal bancaria para realizar ese procedimiento.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00124-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00124-01.pdf

8FPH20-00125-01 CSIRT ADVIERTE DE PHISHING DE SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00125-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Marzo de 2020
Última revisión	04 de Marzo 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 que tienen contratado el servicio streaming de Netflix.

El correo indica que existe un inconveniente con la información de pago. La modalidad de estafa en este caso es ofrecer varias alternativas al usuario, desde ir a un centro de ayudas, contactarse con la empresa, ofrece un nuevo intento o ingresar a la nueva forma de pago. Cada alternativa lleva a la víctima hacia un enlace que se asemeja al sitio de Netflix. En ese sitio se solicita a las víctimas los datos de sus cuentas de usuario y luego los datos de la tarjeta de crédito.

Enlace:

https://www.csirt.gob.cl/alertas/8fph20-00125-01/
https://www.csirt.gob.cl/media/2020/03/8FPH20-00125-01.pdf

Vulnerabilidades

9VSA20-00148-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PHP

Alerta de seguridad informática	9VSA20-00148-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Febrero de 2020
Última revisión	27 de Febrero de 2020

Vulnerabilidad

CVE-2020-7061
CVE-2020-7062
CVE-2020-7063

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de PHP, referente a múltiples vulnerabilidades que afectan a PHP, las cuales de ser explotadas permitirían a un atacante gatillar errores en memoria permitiendo obtener información potencialmente sensible, generar ataques de denegación de servicios y hasta comprometer completamente al sistema afectado.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00148-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00148-01.pdf

9VSA20-00149-01 CSIRT COMPARTE ACTUALIZACIÓN PARA PLATAFORMA DE MISP

Alerta de seguridad informática	9VSA20-00149-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Febrero de 2020
Última revisión	28 de Febrero de 2020

Vulnerabilidad

CVE-2020-8890
CVE-2020-8891
CVE-2020-8892
CVE-2020-8893
CVE-2020-8894

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del repositorio oficial de MISP, referente a múltiples vulnerabilidades que afectan a su plataforma, las cuales permitirían a un atacante remoto realizar ataques XSS, obtener acceso a

funcionalidades no autorizadas, evadir medidas de seguridad y realizar ataques de fuerza bruta. Este informe incluye su respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00149-01/
https://www.csirt.gob.cl/media/2020/02/9VSA20-00149-01.pdf

9VSA20-00150-01 CSIRT COMPARTE ACTUALIZACIONES DE GOOGLE PARA CHROME

Alerta de seguridad informática	9VSA20-00150-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Marzo de 2020
Última revisión	04 de Marzo de 2020

Vulnerabilidad

CVE-2020-6420

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google referente a vulnerabilidades presentes en el navegador Chrome.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00150-01/
https://www.csirt.gob.cl/media/2020/03/9VSA20-00150-01.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
167.172.137.163	Port Scan
192.241.221.83	Port Scan
192.241.213.126	Port Scan
198.199.119.146	Port Scan
107.173.140.108	Port Scan
192.241.237.194	Port Scan
192.241.224.136	Port Scan
192.241.214.114	Port Scan
192.241.206.126	Port Scan
162.243.135.230	Port Scan

162.243.133.139	Port Scan
115.195.209.12	DDoS
125.104.198.109	DDoS
185.81.157.124	Port Scan
192.241.226.132	Port Scan
208.97.136.124	Port Scan
192.241.226.154	Port Scan
162.243.134.205	Port Scan
103.210.21.207	Port Scan
122.114.11.28	Hacking
80.82.77.86	Hacking
162.243.134.173	Port Scan
202.79.24.71	Port Scan
85.33.36.165	Hacking
3.125.34.242	Hacking
178.61.100.162	Hacking
223.18.138.237	Hacking
185.139.48.130	Hacking
128.199.253.208	Hacking
195.154.255.107	Port Scan
54.39.224.228	Port Scan
79.124.56.226	Port Scan
159.89.180.144	Port Scan
162.243.135.85	Port Scan
165.22.208.167	DDoS
162.243.135.240	Port Scan
162.243.134.175	Port Scan
116.87.180.192	Port Scan
192.241.213.94	Port Scan
45.58.148.50	Port Scan
192.241.231.159	Port Scan
172.86.125.166	Port Scan
192.241.214.158	Port Scan
42.190.151.78	Port Scan
222.164.207.16	Port Scan
116.86.192.212	Port Scan
162.243.134.233	Port Scan
192.241.235.228	Port Scan
192.241.194.198	Port Scan
192.241.203.178	Port Scan
77.247.110.168	Port Scan

192.241.238.166	Port Scan
192.241.217.113	Port Scan
192.241.195.42	Port Scan
192.241.224.90	Port Scan
162.243.132.79	Port Scan
192.241.239.181	Port Scan
103.207.38.221	Port Scan
45.143.221.46	Port Scan
162.255.117.28	Port Scan
192.241.230.223	Port Scan
162.243.135.165	Port Scan
192.241.211.138	Port Scan
192.119.9.62	Port Scan
37.49.230.26	Port Scan
58.151.241.180	Port Scan
192.241.237.71	Port Scan
46.101.232.43	Malware
213.136.85.27	Malware
162.243.132.251	Port Scan
192.241.207.175	Port Scan
192.241.225.157	Port Scan
162.243.134.17	Port Scan
192.241.234.173	Port Scan
192.241.213.169	Port Scan
192.241.208.155	Port Scan
45.143.220.228	Port Scan
162.243.135.50	Port Scan
45.227.253.54	Hacking
162.243.133.200	Port Scan
137.59.253.54	Port Scan
162.243.135.231	Port Scan
185.183.105.188	Port Scan
79.119.125.39	Port Scan
93.13.160.211	Port Scan
122.252.107.214	Port Scan
192.99.110.151	Port Scan
37.49.226.13	Port Scan
162.243.132.164	Port Scan
192.241.195.168	Port Scan
192.241.198.89	Port Scan
192.241.222.84	Port Scan

192.241.222.128	Port Scan
46.105.236.211	Port Scan
192.241.202.102	Port Scan
5.152.205.152	Port Scan
45.143.220.212	Port Scan
45.143.220.230	Port Scan
69.163.46.100	Port Scan
139.59.95.238	Port Scan
163.197.192.37	Port Scan
185.53.88.125	Port Scan
186.233.185.16	Port Scan
192.241.213.79	Port Scan
192.241.215.149	Port Scan
192.241.224.239	Port Scan
192.241.227.56	Port Scan
192.241.231.129	Port Scan
78.128.112.14	Port Scan
192.241.215.188	Port Scan
192.241.229.55	Port Scan
192.241.194.63	Port Scan
192.241.222.126	Port Scan
192.241.231.128	Port Scan
185.252.30.184	Port Scan
192.241.195.196	Port Scan
192.241.196.66	Port Scan
192.241.209.126	Port Scan
192.241.210.123	Port Scan
192.241.221.126	Port Scan
192.241.227.73	Port Scan
45.83.42.102	Port Scan
192.81.212.37	Port Scan
111.26.185.208	Hacking
111.230.249.181	Hacking
49.235.81.41	Hacking
129.28.172.153	Hacking
192.241.225.143	Port Scan
192.241.215.57	Port Scan
192.241.223.141	Port Scan
192.241.224.206	Port Scan
192.241.229.242	Port Scan
192.241.226.84	Port Scan

192.241.218.63	Port Scan
192.241.233.88	Port Scan
192.241.211.209	Port Scan
192.241.219.64	Port Scan
192.241.205.120	Port Scan
192.241.212.115	Port Scan
192.241.230.80	Port Scan
192.241.222.137	Port Scan
192.241.230.202	Port Scan
192.241.218.25	Port Scan
192.241.208.140	Port Scan
178.238.8.211	Port Scan
192.241.214.162	Port Scan
62.171.135.80	Port Scan
192.241.218.130	Port Scan
192.241.230.151	Port Scan
192.241.230.151	Port Scan
209.160.117.174	DDoS
192.241.205.25	Port Scan
62.219.50.248	Port Scan
192.241.213.81	Port Scan
192.241.216.31	Port Scan
192.241.220.149	Port Scan
192.241.222.239	Port Scan
192.241.211.15	Port Scan
192.241.224.49	Port Scan
192.241.231.241	Port Scan
185.39.10.10	Port Scan
192.241.223.212	Port Scan
192.241.214.242	Port Scan
192.241.223.142	Port Scan
192.241.235.84	Port Scan
5.135.232.197	Port Scan
192.241.234.58	Port Scan
192.241.221.199	Port Scan
192.241.231.231	Port Scan
192.241.233.188	Port Scan
192.241.235.46	Port Scan
192.241.220.109	Port Scan
81.177.32.12	Port Scan
81.177.143.31	Port Scan

192.241.226.87	Port Scan
192.241.229.25	Port Scan
192.241.211.170	Port Scan
192.241.227.72	Port Scan
192.241.211.144	Port Scan
220.132.218.44	Hacking
103.84.88.35	Hacking
103.144.241.28	Hacking
192.241.223.178	Port Scan
192.241.209.175	Port Scan
192.241.225.90	Port Scan
192.241.230.65	Port Scan
192.241.234.7	Port Scan
192.241.224.158	Port Scan
128.201.182.71	Port Scan
177.54.131.3	Port Scan
188.25.196.174	Port Scan
192.241.225.122	Port Scan
27.125.148.177	Port Scan
192.241.220.29	Port Scan
192.241.225.20	Port Scan
192.241.205.43	Port Scan
192.241.233.245	Port Scan
192.241.233.247	Port Scan
137.74.105.13	Malware
185.173.105.121	Malware
42.200.79.135	Malware
166.62.126.35	Malware
192.241.205.109	Port Scan
192.241.219.99	Port Scan
192.241.227.234	Port Scan
192.241.228.204	Port Scan
91.212.38.210	Port Scan
192.241.218.78	Port Scan
192.241.219.217	Port Scan
192.241.230.215	Port Scan
192.241.209.152	Port Scan
192.241.218.93	Port Scan
192.241.227.131	Port Scan
198.199.105.134	Port Scan
192.241.209.118	Port Scan

192.241.233.252	Port Scan
192.241.229.52	Port Scan
192.241.230.228	Port Scan
192.241.225.141	Port Scan
192.241.219.53	Port Scan
192.241.230.17	Port Scan
192.241.217.6	Port Scan
192.241.230.149	Port Scan
192.241.221.78	Port Scan
192.241.226.5	Port Scan
192.241.235.132	Port Scan
23.96.85.61	Port Scan
94.102.51.8	Port Scan
134.119.217.78	Port Scan
162.243.132.203	Port Scan
162.243.132.62	Port Scan
162.243.135.153	Port Scan
192.241.234.88	Port Scan
132.148.25.191	Port Scan
103.82.235.2	Port Scan
5.9.87.222	Port Scan
217.61.63.245	Port Scan
183.192.202.12	DDoS
183.232.96.140	DDoS
120.204.1.10	DDoS
125.104.199.151	DDoS
115.196.166.175	DDoS
220.184.109.102	DDoS
192.241.224.137	Port Scan
192.241.225.139	Port Scan
80.202.33.191	Hacking
104.18.49.162	Phishing

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.

- Angelo Saavedra Lienan
- Francisco Torrijos Jaime

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: 2020.03.06 10:18:59 -03'00'