CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Sábado 25 de Enero de 2020

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 16 de y el miércoles 22 de Enero de 2020.

Falsificación de Registro o Identidad

8FFR20-00183-01 CSIRT ADVIERTE DE 8 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00183-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Enero de 2020
Última revisión	16 de Enero 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://csirt.gob.cl/alertas/8ff20-00183-01/

https://csirt.gob.cl/media/2020/01/8FFR20-00183-01.pdf

8FFR20-00184-01 CSIRT ADVIERTE DE 8 SITIOS BANCARIOS FRAUDULENTOS ASOCIADOS A DOS IPS

Alerta de seguridad informática	8FFR20-00184-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Enero de 2020
Última revisión	16 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de 8 portales fraudulentos asociados a una IP que suplantan 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://csirt.gob.cl/alertas/8ffr20-00184-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00184-01.pdf

8FFR20-00185-01 CSIRT ADVIERTE DE SEIS PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00185-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Enero de 2020
Última revisión	17 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de sies portales fraudulentos asociados a cuatro 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://csirt.gob.cl/alertas/8ffr20-00185-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00185-01.pdf

8FFR20-00186-01 CSIRT ADVIERTE DE DOS SITIOS FRAUDULENTOS ASOCIADOS A DOS IPS

Alerta de seguridad informática	8FFR20-00186-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Enero de 2020
Última revisión	18 de Enero 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 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://csirt.gob.cl/alertas/8ffr20-00186-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00186-01.pdf

8FFR20-00187-01 CSIRT ADVIERTE DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR20-00187-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2020
Última revisión	22 de Enero de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres 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://csirt.gob.cl/alertas/8ffr20-00187-01/
https://csirt.gob.cl/media/2020/01/8FFR20-00187-01.pdf

8FPH20-00093-01 CSIRT ADVIERTE PHISHING POR ACTUALIZACIÓN EN SERVIDORES DE CORREO ZIMBRA

Alerta de seguridad informática	8FPH20-00093-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Enero de 2020
Última revisión	16 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 que intenta engañar a los usuarios del correo electrónico corporativo Zimbra.

El correo informa sobre una supuesta actualización del sistema y mantención, el atacante disponibiliza un enlace que es dirigido a un sitio falso del correo corporativo donde se le solicita el nombre de usuario y contraseña.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00093-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00093-01.pdf

8FPH20-00094-01 CSIRT ADVIERTE CAMPAÑA DE PHISHING PARA SERVICIO DE STREAMING

Alerta de seguridad informática	8FPH20-00094-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Enero de 2020
Última revisión	17 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 inconveniente en el medio utilizado para el pago del servicio. 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 de Netflix. En ese sitio se solicita a las víctimas los datos de sus cuentas y luego los datos de la tarjeta de crédito.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00094-01/

https://csirt.gob.cl/media/2020/01/8FPH20-00094-01.pdf

8FPH20-00095-01 CSIRT ADVIERTE DE PHISHING POR RETENCIÓN DE FONDOS

Alerta de seguridad informática	8FPH20-00095-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Enero de 2020
Última revisión	20 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 dirigido a clientes del Banco Scotiabank. En el mensaje los atacantes informan sobre una transferencia de fondos supuestamente retenida desde su cuenta. El phishing trata de persuadir a los usuarios que revisan su estado de cuenta de acceder 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://csirt.gob.cl/alertas/8fph20-00095-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00095-01.pdf

8FPH20-00096-01 CSIRT ADVIERTE DE PHISHING EN CORREO CORPORATIVO

Alerta de seguridad informática	8FPH20-00096-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Enero de 2020
Última revisión	20 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 que intenta engañar a usuarios del correo electrónico corporativo Microsoft Outlook Web Access 2020.

El mensaje informa que se realizó una actualización de los sistemas de correo, acción que genera más espacio de almacenamiento y un acceso más fácil. El atacante disponibiliza un enlace que dirige a un sitio falso de correo corporativo donde se le solicita el nombre de usuario y contraseña.

Enlace:

https://csirt.gob.cl/alertas/8fph20-00096-01/
https://csirt.gob.cl/media/2020/01/8FPH20-00096-01.pdf

9VSA20-00124-01 CSIRT COMPARTE ACTUALIZACIÓN PARA WIRESHARK

Alerta de seguridad informática	9VSA20-00124-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Enero de 2020
Última revisión	16 de Enero de 2020

Vulnerabilidad

CVE-2020-7044
CVE-2020-7045

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Wireshark, referente a vulnerabilidades que afectan a su analizador de paquetes, las cuales de ser explotadas permitirían a un atacante remoto realizar ataques de denegación de servicios sobre los sistemas vulnerables. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00124-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00124-01.pdf

9VSA20-00125-01 CSIRT COMPARTE ACTUALIZACIONES DE FOXIT PARA FOXIT READER Y PHANTOMPDF

Alerta de seguridad informática	9VSA20-00125-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Enero de 2020
Última revisión	17 de Enero de 2020

Vulnerabilidad

CVE-2019-5130
CVE-2019-5145
CVE-2019-5131
CVE-2019-5126

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Foxit, referente a vulnerabilidades que afectan a Foxit Reader y PhantomPDF, las cuales de ser explotadas permitirían a un atacante remoto realizar ataques de corrupción de memoria comprometiendo al sistema vulnerable. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00125-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00125-01.pdf

9VSA20-00126-01 CSIRT COMPARTE ACTUALIZACIONES PARA MICROSOFT INTERNET EXPLORER

Alerta de seguridad informática	9VSA20-00126-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de enero de 2020
Última revisión	20 de enero de 2020

Vulnerabilidad

CVE-2020-0674

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft referente a una vulnerabilidad de corrupción de memoria presente en el motor de secuencias de comandos de Microsoft Internet Explorer el cual puede permitir que un atacante remoto no autenticado ejecute código arbitrario.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00126-01/
https://csirt.gob.cl/media/2020/01/9VSA20-00126-01.pdf

9VSA20-00108-02 CSIRT COMPARTE NUEVA ACTUALIZACIÓN PARA PRODUCTOS CITRIX

Alerta de seguridad informática	9VSA20-00108-02
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2020
Última revisión	21 de enero de 2020

Vulnerabilidad

CVE-2019-19781

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Citrix, referente a una vulnerabilidad que afecta sus productos Citrix ADC, Citrix Gateway y Citrix SD-WAN WANOP, los cuales de ser explotados, permitirían a un atacante realizar la ejecución de código remoto sobre el sistema afectado. Este informe incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa20-00108-02/
https://csirt.gob.cl/media/2020/01/9VSA20-00108-02.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
117.150.42.185	DdoS
59.61.174.213	DdoS
119.165.185.169	DdoS
116.112.206.245	DdoS
111.25.63.194	DdoS
60.208.206.151	DdoS
222.41.65.249	DdoS
119.0.21.141	DdoS
180.168.189.19	DdoS
101.87.157.185	DdoS
51.254.4.226	Port Scan
58.56.46.98	DdoS
120.239.43.88	DdoS
113.105.135.20	DdoS
111.18.94.107	DdoS
220.173.201.53	DdoS
125.42.214.239	DdoS
58.57.35.18	DdoS
58.62.112.156	DdoS
114.92.43.11	DdoS
123.166.77.82	DdoS
45143220160	Port Scan
89.38.145.5	Port Scan
195.154.62.3	Port Scan
61.220.50.173	Port Scan
212.237.47.190	Port Scan
174.138.56.164	Port Scan
182.222.119.174	Port Scan
185.112.82.26	Port Scan
117.216.172.130	Port Scan
49.35.94.13	Port Scan
190.107.177.251	Phishing
61.2.22.171	Port Scan
80.121.70.64	Port Scan

95.14.67.88	Port Scan
178.130.73.231	Port Scan
128.204.218.69	Port Scan
185.53.91.28	Port Scan
144.91.116.157	Port Scan
183.83.38.168	Port Scan
144.91.86.28	Port Scan
188.25.151.203	Port Scan
58.182.142.32	Port Scan
188.194.166.192	Port Scan
79.117.237.64	Port Scan
116.86.160.252	Port Scan
113.160.225.142	Port Scan
103.253.42.51	Port Scan
125.93.83.105	DdoS
42.91.175.140	DdoS
115.171.132.47	DdoS
61166244190	DdoS
223.80.238.23	DdoS
124.226.157.194	DdoS
182.200.0.188	DdoS
110.244.187.106	DdoS
42.102.34.180	DdoS
113.232.50.222	DdoS
80.211.11.4	Port Scan
163.172.116.24	Port Scan
116.58.244.175	Port Scan
212.237.47.182	Port Scan
144.217.234.243	Port Scan
86.183.96.2	Port Scan
163.172.53.65	Port Scan
194.26.69.101	Port Scan
194.26.69.104	Port Scan
222.158.101.91	Port Scan
78.100.194.80	Port Scan
85.75.136.76	Port Scan
206.189.139.122	DdoS
216.52.161.1	DdoS
205.242.92.2	DdoS
211.167.241.234	DdoS
63.130.83.36	DdoS

121.40.12.112	DdoS
211.167.241.238	DdoS
39.97.227.18	DdoS
195.129.12.122	DdoS
39.97.162.23	DdoS
39.97.244.100	DdoS
205.242.92.2	DdoS
63.130.83.36	DdoS
216.52.161.1	DdoS
211.167.241.242	DdoS
211.167.241.238	DdoS
211.167.241.234	DdoS
195.129.12.122	DdoS
39.97.162.23	DdoS
39.97.243.165	DdoS
202.183.152.113	DdoS
92.118.38.40	Port Scan
94.130.9.133	Port Scan
212.237.44.187	Port Scan
181.118.173.144	DdoS
182.253.62.121	Port Scan
176.107.133.245	Port Scan
212.83.180.233	Port Scan
113.163.213.186	Port Scan
89.144.47.249	Port Scan
141.98.10.129	Port Scan
37.49.230.37	Port Scan
84.54.113.246	Port Scan
113.161.51.20	Port Scan
1.82.227.193	DdoS
101.80.164.161	DdoS
101.87.197.178	DdoS
101.88.120.62	DdoS
106.122.219.162	DdoS
106.47.154.125	DdoS
110.184.67.247	DdoS
110.53.234.201	DdoS
110.88.213.167	DdoS
111.174.77.71	DdoS
111.18.123.198	DdoS
101.80.164.161	DdoS

111.193.206.39	DdoS
111.194.49.209	DdoS
111.202.190.6	DdoS
111.205.14.30	DdoS
111.29.117.253	DdoS
111.37.49.34	DdoS
112.11.44.172	DdoS
112.12.158.86	DdoS
112.6.33.90	DdoS
223.12.226.60	DdoS
111.19.93.201	DdoS
180.171.140.160	DdoS
203.93.125.30	DdoS
115.78.225.151	Port Scan
163.172.117.190	Port Scan
104.244.77.47	Port Scan
112.22.241.30	DdoS
112.236.240.5	DdoS
112.28.212.152	DdoS
112.3.253.47	DdoS
112.37.211.105	DdoS
163.172.11.172	Port Scan
23.94.184.118	Port Scan
89.144.47.249	Port Scan
89248174146	Port Scan
103.99.3.10	Port Scan
59.12.215.20	Port Scan
218.108.29.146	DdoS
218.81.18.31	DdoS
220.164.67.91	DdoS
220.173.127.19	DdoS
220.184.162.34	DdoS
221.197.50.29	DdoS
222.182.12.202	DdoS
222.214.233.105	DdoS
222.70.123.32	DdoS
222.94.225.199	DdoS
223.8.91.218	DdoS
223.88.139.63	DdoS
223.89.134.252	DdoS
223.91.23.34	DdoS

27.17.171.7	DdoS
179.107.111.237	Port Scan
178.239.161.253	Port Scan
173.249.56.119	Port Scan
27.255.77.246	Port Scan
74.91.124.72	Port Scan
115.124.69.198	Port Scan
113.124.69.198	Port Scan
37.237.203.41	Port Scan
167.172.234.5	Port Scan
45134179243	Port Scan
49.247.132.79	Port Scan
157.230.128.195	Port Scan
51.91.102.120	Port Scan
104.243.38.169	Port Scan
79.124.49.229	Port Scan
5.62.16.32	Port Scan
115.195.208.82	Port Scan
183.91.2.37	Port Scan
212.47.232.148	Port Scan
179.182.142.138	Port Scan
41.140.137.40	Port Scan
51.77.212.188	Port Scan
206.189.147.118	Port Scan
167.172.19.150	DdoS
198.50.250.134	Port Scan
45143220171	Port Scan
86.73.196.126	Port Scan
210.211.117.135	Port Scan
103.193.129.121	Port Scan
14.186.254.60	Port Scan
27.17.191.201	DdoS
27.18.88.230	DdoS
27.213.46.200	DdoS
27.224.68.56	DdoS
27.38.242.116	DdoS
39.128.119.39	DdoS
39129161172	DdoS
39.149.50.19	DdoS
39.165.55.152	DdoS
39.165.55.172	DdoS

39170197181	DdoS
39.182.214.80	DdoS
39188128232	DdoS
39.68.45.214	DdoS
79.137.118.81	Port Scan
83.97.20.33	Port Scan
172.105.71.24	Port Scan
39.70.179.7	DdoS
42.101.116.108	DdoS
43.230.144.55	DdoS
49.74.36.62	DdoS
49.79.191.153	DdoS
49.80.125.145	DdoS
58.100.22.110	DdoS
58212132119	DdoS
58.253.37.238	DdoS
58.49.165.52	DdoS
59.55.120.16	DdoS
60.177.168.8	DdoS
60.221.121.249	DdoS
61.130.74.142	DdoS
61.163.47.46	DdoS
61.242.32.18	DdoS
82149194134	DdoS
95.211.190.243	Port Scan
51.89.99.155	Port Scan
54.36.131.232	Port Scan
41.141.85.195	Port Scan
62.210.22.57	Port Scan
62.210.222.57	Port Scan
188.40.66.118	Port Scan
180.247.132.85	Port Scan
172.104.149.176	Port Scan
172.105.92.229	Port Scan
185.208.211.168	Port Scan
89.34.27.23	Port Scan
51.89.157.32	Port Scan
79.124.62.18	Port Scan
195.154.63.224	Port Scan
162.241.60.80	Phishing
36.65.134.241	Port Scan

162.241.60.178	Phishing
178.33.34.78	Port Scan
37.49.230.108	Port Scan
69.70.75.46	Port Scan
193.56.28.130	Port Scan
47.89.50.166	Port Scan
58.96.211.85	Port Scan
79.117.11.86	Port Scan
141.98.10.47	Port Scan
119.179.16.31	DdoS
182.126.21.1	DdoS
113.77.137.238	DdoS
116.27.145.2	DdoS
101.80.89.45	DdoS
59.63.178.76	DdoS
106.91.204.113	DdoS
117.173.197.254	DdoS
60.191.10.162	DdoS
223.64.181.45	DdoS
103.5.144.42	Port Scan
92.118.38.56	Port Scan
144.91.127.211	Port Scan
45.56.72.235	Port Scan
108.183.170.108	Port Scan
66.96.147.144	Malware
107.174.24.112	Phishing
218.189.15.78	Port Scan
159.65.158.74	Phishing
142.93.226.63	Phishing
27.72.43.83	Port Scan
45.148.10.184	Port Scan
45.125.66.124	Port Scan
138.128.182.130	Phishing
93.186.251.216	Phishing
145.239.149.217	Port Scan
45.143.220.169	Port Scan
117.2.49.82	Port Scan
103.145.255.113	Port Scan
89.34.27.135	Port Scan
195.231.1.214	Port Scan
154.16.67.155	Port Scan

128.90.113.124	DdoS
185.220.101.79	DdoS
189.203.187.59	DdoS
89.39.107.201	DdoS
210.116.77.218	Port Scan
185.53.88.116	Port Scan
37.49.230.109	Port Scan
203.155.52.7	Malware
45.164.124.108	Port Scan
189.1.170.174	Port Scan
24.5.7.236	Port Scan
80.211.55.90	Malware
96.79.137.178	Malware
216.83.52.60	Malware
103.118.222.83	Malware
194.180.225.23	Port Scan
51.88.206.211	Port Scan
45.10.175.13	Malware
185.29.70.97	Port Scan
178.62.206.245	DdoS
144.208.127.181	Phishing
213.199.180.175	Phishing
41.90.110.86	Port Scan
94.102.57.241	Port Scan
156.96.56.141	Port Scan
103.99.1.31	Port Scan
104.248.13.98	Port Scan
160.153.129.228	Phishing
45.143.220.167	Port Scan
154.231.105.243	Port Scan
185.29.120.154	Port Scan
92.118.160.21	Port Scan
63.143.45.26	Port Scan
185.246.130.8	Port Scan
192.99.154.51	Port Scan
92.118.160.13	Port Scan
185.246.130.5	Port Scan
121.88.5.176	Port Scan
173.239.37.163	Port Scan
84.56.81.13	Port Scan
134.209.145.227	Port Scan

83.97.20.55	Port Scan
107.189.10.185	Port Scan
79.114.231.198	Port Scan
177.72.43.99	Port Scan
42.191.45.59	Port Scan
58.182.172.231	Port Scan
58.182.2.49	Port Scan
83.97.20.54	Port Scan
85.190.148.140	Port Scan
185.53.88.118	Port Scan
210.119.238.200	Port Scan
141.98.80.69	Port Scan
156.210.39.42	Port Scan
116.204.154.13	Port Scan
117.211.106.230	Port Scan
200.188.6.177	Port Scan
51.79.102.96	Port Scan
216.245.197.14	Port Scan
5.202.147.121	Port Scan
36.65.121.138	Port Scan
212.42.106.90	Port Scan
200.54.255.253	Port Scan
60.176.209.187	DdoS
125.122.214.61	DdoS
122.227.116.79	DdoS
122.246.101.134	DdoS
123.96.232.224	DdoS
89.34.27.62	Port Scan
68.183.170.50	Port Scan
64.39.99.234	Port Scan
121.101.134.124	Port Scan
121.101.134.125	Port Scan
121.101.134.126	Port Scan
121.101.134.127	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.

- Gustavo Galleguillos
- Eduardo Aceto
- Rodrigo Jiménez
- Bernardo Avilés

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: 2020.01.25 14:31:18 -03'00'