13BCS-00034-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 27 de Diciembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 19 y el miércoles 25 de Diciembre.

Falsificación de Registro o Identidad

8FFR-00156-001 CSIRT ADVIERTE LA ACTIVACIÓN DE DOS SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00156-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial de 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/8ffr-00156-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00156-001.pdf

8FFR-00157-001 CSIRT ADVIERTE ACTIVACIÓN DE DOS PORTALES BANCARIOS FRAUDULENTOS PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00157-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a una IP que suplantan el sitio web oficial del Banco Santander, 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/8ffr-00157-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00157-001.pdf

8FFR-00158-001 CSIRT ADVIERTE ACTIVACIÓN DE TRES PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00158-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de tres portales fraudulentos asociados a una 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/8ffr-00158-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00158-001.pdf

8FFR-00159-001 CSIRT ADVIERTE DE PORTAL BANCARIO FRAUDULENTO PARA ROBO DE CREDENCIALES

Alerta de seguridad informática	8FFR-00159-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2019
Última revisión	20 de diciembre 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 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 del servicio y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00159-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00159-001.pdf

8FFR-00160-001 CSIRT ADVIERTE ACTIVACIÓN DE 6 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00160-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2019
Última revisión	20 de diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de sies portales fraudulentos asociados a una IP que suplantan el sitio web oficial de 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/8ffr-00160-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00160-001.pdf

8FFR-00161-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00161-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2019
Última revisión	21 de diciembre 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 de 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 y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00161-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00161-001.pdf

8FFR-00162-001 CSIRT ADVIERTE ACTIVACIÓN DE TRES SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00162-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de diciembre de 2019
Última revisión	24 de diciembre 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 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/8ffr-00162-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00162-001.pdf

8FFR-00163-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00163-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de diciembre de 2019
Última revisión	24 de diciembre 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 de 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 y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00163-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00163-001.pdf

8FFR-00164-001 CSIRT INFORMA ACTIVACIÓN DE PORTAL BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00164-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de diciembre de 2019
Última revisión	24 de diciembre 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 de Banco de Chile, 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 y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00164-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00164-001.pdf

8FFR-00165-001 CSIRT ADVIERTE DE SITIO FRAUDULENTO PARA ROBO DE CREDENCIALES BANCARIAS

Alerta de seguridad informática	8FFR-00165-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de diciembre de 2019
Última revisión	25 de diciembre 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 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 y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00165-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00165-001.pdf

Vulnerabilidades

9VSA-00103-001 CSIRT COMPARTE ACTUALIZACIONES PARA JOOMLA

Alerta de seguridad informática	9VSA-00103-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 de diciembre de 2019

Vulnerabilidad

CVE-2019-19845
CVE-2019-19846

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por Joomla referente a vulnerabilidades que afectan a su gestor de contenidos Joomla!, esto junto a sus respectivas mitigaciones.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00103-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00103-001.pdf

9VSA-00104-001 CSIRT COMPARTE ACTUALIZACIÓN PARA DJANGO

Alerta de seguridad informática	9VSA-00104-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2019
Última revisión	20 de diciembre de 2019

Vulnerabilidad

CVE-2019-19844

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por Django referente a una vulnerabilidad que afecta su marco de desarrollo de aplicaciones web. El informe también contiene los enlaces para descargar las respectivas mitigaciones.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00104-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00104-001.pdf

9VSA-00105-001 CSIRT COMPARTE ACTUALIZACIONES PARA VMWARE

Alerta de seguridad informática	9VSA-00105-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2019
Última revisión	20 de diciembre de 2019

Vulnerabilidad

CVE-2019-5539

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por VMware, referente a una vulnerabilidad de tipo escalación de privilegios, que afecta a dos de sus productos, esto junto a sus respectivas mitigaciones.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa-00105-001/
https://csirt.gob.cl/media/2019/12/9VSA-00105-001.pdf

9VSA-00106-001 CSIRT COMPARTE ACTUALIZACIÓN PARA WORDPRESS

Alerta de seguridad informática	9VSA-00106-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Diciembre de 2019
Última revisión	21 de Diciembre de 2019

Vulnerabilidad

CVE-2019-19915

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de múltiples fuentes referente a vulnerabilidades que afectan al plugin '301 Redirects – Easy Redirect Manager' para WordPress. Este reporte incluye la respectiva mitigación.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00106-001/
https://csirt.gob.cl/media/2019/12/9VSA-00106-001.pdf

9VSA-00107-001 CSIRT COMPARTE ACTUALIZACIONES PARA BIG-IP(LTM) DE F5

Alerta de seguridad informática	9VSA-00107-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Diciembre de 2019
Última revisión	21 de Diciembre de 2019

Vulnerabilidad

CVE-2019-6681

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información entregada por F5 referente a una vulnerabilidad que afecta a su producto BIG-IP(LTM). El informe también incluye la respectiva actualización.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa-00107-001/
https://csirt.gob.cl/media/2019/12/9VSA-00107-001.pdf

9VSA-00108-001 CSIRT COMPARTE ACTUALIZACIÓN PARA PRODUCTOS CITRIX

Alerta de seguridad informática	9VSA-00108-001

Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Diciembre de 2019
Última revisión	21 de Diciembre de 2019

Vulnerabilidad

CVE-2019-19781

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida de Citrix referente a una vulnerabilidad crítica que afecta a sus productos, la cual, de ser explotada, permitiría a un atacante remoto acceder a la red local de la víctima. El documento también incluye la respectiva mitigación.

Enlace

https://csirt.gob.cl/vulnerabilidades/9vsa-00108-001/
https://csirt.gob.cl/media/2019/12/9VSA-00108-001.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
45.227.255.224	Port Scan
191.243.156.114	Port Scan
62.210.143.213	Port Scan
94.174.93.27	Port Scan
94.174.93.72	Port Scan
80.82.65.88	Port Scan
45.55.35.47	Port Scan
31.14.40.166	Port Scan
80.82.70.225	Port Scan
190.100.118.27	DDoS
190.151.108.235	DDoS
1.161.220.135	Port Scan
186.67.93.27	Port Scan
185.61.137.172	Port Scan
186.236.30.246	Port Scan
167.249.245.44	Port Scan

45.189.74.190	Port Scan
46.166.187.188	Port Scan
58.182.72.135	Port Scan
68.183.109.133	Port Scan
103.25.3.100	Port Scan
113.174.33.97	Port Scan
162.208.51.18	Port Scan
163.172.6.250	Port Scan
178.79.140.186	Port Scan
185.153.196.8	Port Scan
156.236.99.158	Port Scan
163.172.6.251	Port Scan
45.136.108.164	Port Scan
177.54.144.67	Port Scan
79.124.62.34	Port Scan
51.255.237.84	Port Scan
66.175.56.96	Port Scan
64.39.99.94	Port Scan
80.82.65.82	Port Scan
103.133.107.217	Port Scan
80.82.70.211	Port Scan
195.154.226.126	Port Scan
121.7.25.226	Port Scan
222.254.18.93	Port Scan
79.255.191.214	Port Scan
185.198.56.93	Port Scan
42.114.199.251	Port Scan
195.231.9.220	Port Scan
185.200.118.55	Port Scan
46.101.116.48	Port Scan
14.172.3.67	Port Scan
171.238.39.232	Port Scan
103.82.158.99	Port Scan
163.172.204.66	Port Scan
87.122.110.65	Port Scan
217.61.60.65	Port Scan
45.148.10.188	Port Scan
89.248.160.150	Port Scan
93.174.93.195	Port Scan
94.102.56.215	Port Scan
185.35.64.187	Port Scan

190.5.48.95	DDoS
103.125.191.106	Port Scan
162.244.81.224	Port Scan
78.46.123.33	Port Scan
68.183.165.141	Port Scan
107.148.208.166	Port Scan
24.155.189.235	Port Scan
185.216.140.185	Port Scan
103.79.143.196	Port Scan
80.82.70.34	Port Scan
77.247.109.92	Port Scan
68.183.101.113	Port Scan
82.118.242.108	Port Scan
185.153.196.225	Port Scan
185.153.199.208	Port Scan
218.211.168.180	Port Scan
121.7.25.224	Port Scan
1.54.198.211	Port Scan
163.47.87.26	Port Scan
193.56.28.33	Port Scan
45.67.14.150	Port Scan
51.38.93.221	Port Scan
104.244.73.31	Port Scan
115.78.226.69	Port Scan
118.70.12.170	Port Scan
122.154.42.38	Port Scan
185.175.93.34	Port Scan
185.198.58.88	Port Scan
37.49.230.101	Port Scan
45.76.232.166	Port Scan
45.95.168.116	Port Scan
51.158.90.173	Port Scan
51.158.90.174	Port Scan
51.158.90.179	Port Scan
68.183.105.46	Port Scan
71.199.142.33	Port Scan
79.254.68.220	Port Scan
79.254.81.252	Port Scan
94.23.196.177	Port Scan
107.189.11.160	Port Scan
113.190.246.30	Port Scan

193.56.28.33	Port Scan
87.123.147.227	Port Scan
52.237.52.85	Port Scan
134.236.76.144	Port Scan
159.65.225.148	Port Scan
182.70.203.251	Port Scan
183.81.120.202	Port Scan
185.200.118.43	Port Scan
222.236.107.77	Port Scan
177.12.163.106	Malware
185.156.73.57	Port Scan
68.183.101.42	Port Scan
5.188.206.215	Port Scan
185.234.217.228	Port Scan
142.44.223.234	Port Scan
167.86.110.190	Port Scan
51.255.126.132	Port Scan
145.239.205.133	Port Scan
37.49.230.92	Port Scan
205.185.114.216	Port Scan
125.161.128.80	Port Scan
144.91.75.53	Port Scan
195.22.232.10	Port Scan
45.143.221.33	Port Scan
45.65.49.98	Port Scan
77.243.29.254	Port Scan
89.248.162.171	Port Scan
96.47.239.197	Port Scan
77.247.110.199	Port Scan
93.91.173.109	DDoS
117.88.176.132	DDoS
184.177.112.206	DDoS
90.176.236.40	DDoS
112.109.198.106	DDoS
180.179.98.22	DDoS
119.23.168.1	DDoS
185.45.239.245	DDoS
77.104.70.81	DDoS
210.26.64.44	DDoS
118.89.234.236	DDoS
173.249.35.163	DDoS

91.155.210.126	DDoS
222.95.144.72	DDoS
151.253.165.70	DDoS
39.104.97.42	DDoS
208.255.161.107	DDoS
222.175.171.6	DDoS
140.131.190.110	DDoS
116.48.142.127	DDoS
41.73.9.101	DDoS
36.104.132.31	DDoS
2.50.169.72	DDoS
77.247.110.61	Port Scan
62.210.149.143	Port Scan
23.245.229.59	Port Scan
189.1.172.13	Port Scan
89.40.126.224	Port Scan
77.247.110.60	Port Scan
154.48.248.207	Port Scan
163.172.9.12	Port Scan
163.172.9.13	Port Scan
138.99.216.171	Port Scan
104.203.93.58	Port Scan
68.183.92.202	Phishing
103.79.143.184	Port Scan
85.209.3.0/24	Port Scan
78.8.22.190	Port Scan
171.237.130.166	Port Scan
36.72.216.245	Port Scan
104.244.74.57	Hacking
27.69.250.151	Port Scan
36.70.129.24	Port Scan
103.87.251.102	Port Scan
51.81.112.138	Port Scan
210.48.139.158	Port Scan
125.164.94.177	Port Scan
159.203.193.42	Port Scan
14.232.32.200	Port Scan
122.3.88.168	Port Scan
37.49.230.88	Port Scan
87.123.159.100	Port Scan
80.211.188.62	Port Scan

113.190.46.178	Port Scan
103.216.218.191	Port Scan
68.183.128.201	Port Scan
182.16.20.42	Malware
193.56.28.14	Port Scan
188.165.28.7	Port Scan
188.25.209.155	Port Scan
58.182.86.101	Port Scan
58.182.99.179	Port Scan
58.182.222.173	Port Scan
94.225.234.66	Port Scan
79.115.184.213	Port Scan
78.128.110.139	Port Scan
88.38.118.83	Hacking
163.172.109.61	Port Scan
51.91.20.145	Port Scan
5.196.85.53	Port Scan
35.224.77.140	Port Scan
51.77.111.27	Port Scan
45.58.113.219	Port Scan
213.230.95.110	Port Scan
5.144.132.11	Port Scan
58.65.221.100	Port Scan
159.89.160.91	Port Scan
210.56.16.103	Port Scan
144.91.108.140	Port Scan
162.208.51.37	Port Scan
87.123.157.117	Port Scan
51.89.16.194	Port Scan
58.82.247.199	Port Scan
45.143.220.138	Port Scan
68.183.128.170	Port Scan
151.106.34.187	Port Scan
185.132.53.104	Port Scan
41.226.4.26	Port Scan
193.29.15.86	Port Scan
51.89.228.124	Port Scan
5.226.138.86	Port Scan
45.229.199.39	Port Scan
68.183.119.181	Port Scan
110.173.48.154	Port Scan

144.91.82.7	Port Scan
171.224.181.101	Port Scan
52.128.224.98	Port Scan
196.207.68.13	Port Scan
51.161.105.89	Port Scan
196.240.57.91	Port Scan
91.135.201.122	Port Scan
92.118.37.61	Port Scan
45.143.220.140	Port Scan
185.153.199.201	Port Scan
144.91.103.222	Port Scan
104.199.131.32	Port Scan
45.143.220.136	Port Scan
139.162.162.67	Port Scan
179.8.55.153	Port Scan
185.128.41.50	Port Scan
195.154.26.144	Port Scan
116.86.154.185	Port Scan
79.114.148.117	Port Scan
182.19.218.149	Port Scan
170.231.128.221	Port Scan
101.255.86.41	Port Scan
104.149.170.180	Port Scan
185.73.114.155	Port Scan
45.115.4.242	Port Scan
182.73.3.50	Port Scan
68.183.123.126	Port Scan
193.111.234.47	Port Scan
1.172.172.149	Port Scan
51.68.216.158	Port Scan
54.36.5.221	Port Scan
159.203.90.120	Port Scan
37.99.136.252	Port Scan
65.19.174.198	Port Scan
91.121.179.189	Port Scan
39.32.226.189	Port Scan
188.192.114.55	Port Scan
220.184.67.152	Port Scan
45.148.10.9	Port Scan
51.38.140.18	Port Scan
185.220.100.130	Port Scan

212.47.225.100	Port Scan
109.70.100.65	Port Scan
91.134.185.94	Port Scan
83.224.141.148	DDoS
132.147.36.20	DDoS
162.243.172.134	Phishing
45.67.14.152	Port Scan
45.136.108.128	Port Scan
190.136.175.47	Port Scan
111.91.47.169	Port Scan
142.93.0.252	Port Scan
144.91.82.224	Port Scan
144.91.82.247	Port Scan
194.55.187.3	Port Scan
107.167.2.35	Port Scan
109.160.53.22	Port Scan
163.30.34.20	Port Scan
194.55.187.12	Port Scan
154.125.52.201	Port Scan
118.33.207.180	Port Scan
80.15.207.32	Port Scan
45.128.133.234	Port Scan
185.93.3.92	Port Scan
184.75.210.226	Port Scan
151.106.52.134	Port Scan
82.103.136.16	Port Scan
64.62.243.163	Port Scan
89.163.242.206	Port Scan
142.122.123.229	Port Scan
186.111.171.60	Port Scan
148.255.175.156	Port Scan
69.162.124.230	Port Scan
176.164.51.183	Port Scan
83.224.143.101	Port Scan
210.222.232.207	Port Scan
108.2.217.148	Port Scan
132.147.36.20	Port Scan
156.216.159.163	Port Scan
188.26.119.151	Port Scan
31.5.22.175	Port Scan
79.124.8.19	Port Scan

156.207.215.233	Port Scan
199.191.50.92	Port Scan
144.91.83.19	Port Scan
62.149.158.252	Malware
177.34.32.109	Malware
2.138.111.86	Malware
122.172.96.18	Malware
69.93.243.5	Malware
200.43.183.102	Malware
79.124.76.30	Malware
188.125.166.114	Malware
37.59.52.64	Malware
50.28.35.36	Malware
154.70.39.158	Malware
108.29.37.11	Malware
65.112.218.2	Malware
91.80.137.166	DDoS
118.33.207.32	DDoS
59.1.203.92	Port Scan
1.231.54.59	Port Scan
114.203.42.25	Port Scan
121.168.244.89	Port Scan
121.167.24.23	Port Scan
211.228.59.78	Port Scan
175.195.142.97	Port Scan
121.179.149.182	Port Scan
177.54.137.66	Port Scan
104.200.67.173	Malware
185.82.202.109	Malware
192.52.167.241	Malware

URL	Motivo
bancasbci[.]suscribeterút[.]ml	Phishing
bancasbci[.]xn--suscribetert-wkb[.]ml	Phishing
santanderchile[.]sytes[.]net	Phishing
cuentarut-enlineas.top/imagenes/comun2008	Phishing
https://cmr-enlinea.top/home/	Phishing
benreat.com	Malware
planlamaison.com	Malware
sarymar.com	Malware
teamchuan.com	Malware
c1oudflare.com	Malware
athery.bit	Malware
babloom.bit	Malware
floppys.bit	Malware
hwartless.bit	Malware
foods-pro.com	Malware
dopearos.com	Malware
temerariamente humano.org	Malware
ololo.espacio	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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.27 11:30:10 -03'00'