13BCS-00032-001

CSIRT del Gobierno de Chile

Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicado el Viernes 13 de Diciembre de 2019

Resumen de noticias, reportes, alertas e indicadores de compromisos informados por CSIRT entre el jueves 5 y el miércoles 11 de Diciembre.

Falsificación de Registro o Identidad

8FFR-00140-001 CSIRT ADVIERTE LA ACTIVACIÓN DE CINCO SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00140-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de Diciembre de 2019
Última revisión	5 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cinco 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/8ffr-00140-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00140-001.pdf

8FFR-00141-001 CSIRT INFORMA ACTIVACIÓN DE 3 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00141-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de Diciembre de 2019
Última revisión	5 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 dos IPs que suplantan 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, clientes y a la entidad bancaria aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00141-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00141-001.pdf

8FFR-00142-001 CSIRT ADVIERTE DE 8 SITIOS BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00142-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de Diciembre de 2019
Última revisión	6 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de ocho portales bancarios 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/8ffr-00142-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00142-001.pdf

8FFR-00143-001 CSIRT ADVIERTE DE SIETE PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00143-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de Diciembre de 2019
Última revisión	8 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de siete portales bancarios fraudulentos asociados a tres una 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 del servicio y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00143-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00143-001.pdf

8FFR-00144-001 CSIRT ADVIERTE DE SUPLANTACIÓN DE SITIO DE OPERADOR DE TRAJETAS

Alerta de seguridad informática	8FFR-00144-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Diciembre de 2019
Última revisión	9 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 CMR 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/8ffr-00144-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00144-001.pdf

8FFR-00145-001 CSIRT ADVIERTE DE SEIS PORTALES FRAUDULENTOS QUE INTENTAN SUPLANTAR AL SII

Alerta de seguridad informática	8FFR-00145-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Diciembre de 2019
Última revisión	9 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración del Área de seguridad de Sistemas del Departamento de informática y Aseguramiento de Estándares Tecnológico del Servicio de Impuestos Internos, han identificado la activación de seis portales fraudulentos asociados a una IP que suplantan el sitio web oficial de SII, el que podría servir para robar credenciales de usuarios de esa entidad pública del Estado.
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-00145-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00145-001.pdf

8FFR-00146-001 CSIRT ADVIERTE ACTIVACIÓN DE SITIO BANCARIO FRAUDULENTO

Alerta de seguridad informática	8FFR-00146-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2019
Última revisión	10 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-00146-001/
https://www.csirt.gob.cl/media/2019/12/8FFR-00146-001.docx.pdf

8FFR-00147-001 CSIRT ADVIERTE DE 3 PORTALES BANCARIOS FRAUDULENTOS

Alerta de seguridad informática	8FFR-00147-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Diciembre de 2019
Última revisión	10 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 Itaú, los que podrían servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios y a la entidad aludida.

Enlace:

https://www.csirt.gob.cl/alertas/8ffr-00147-001/

https://www.csirt.gob.cl/media/2019/12/8FFR-00147-001.pdf

Alertas de Phishing

8FPH-00075-001 CSIRT ADVIERTE DE PHISHING EN CORREO ELECTRÓNICO CORPORATIVO

Alerta de seguridad informática	8FPH-00075-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta engañar a los usuarios del correo electrónico corporativo Zimbra.

El correo informa sobre supuestos mensajes bloqueados producto de que el buzón habría sobrepasado el límite de espacio de la cuenta. Los estafadores persuaden al usuario para que seleccione el enlace de “actualizar ahora”. Al seleccionar dicho enlace, la víctima es dirigida a un sitio falso de correo donde se le solicita el nombre de usuario y contraseña.

Enlace

https://www.csirt.gob.cl/alertas/8fph-00075-001/

https://www.csirt.gob.cl/media/2019/12/8FPH-00075-001.docx.pdf

8FPH-00076-001 CSIRT ADVIERTE CAMPAÑAS DE PHISHING BANCARIOS

Alerta de seguridad informática	8FPH-00076-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Scotiabank, para seleccionar un hipervínculo que los direcciona a un sitio semejante al del Banco. Para ello, los atacantes utilizan diversos mensajes en el cuerpo del correo para convencer a la víctima de seleccionar el enlace, cómo por ejemplo:

Que su cuenta se le descontó $300.000 pesos por un incumplimiento de un pago

Que la cuenta fue suspendida por no realizar un pago de impuestos

Que se le descontó $450.000 pesos por un error en los sistemas

Que su tarjeta de crédito por realizar una operación sospechosa se procedió a su bloqueo

Enlace

https://www.csirt.gob.cl/alertas/8fph-00076-001/

https://www.csirt.gob.cl/media/2019/12/8FPH-00076-001.pdf

Alertas de Malware

2CMV-00040-001 CSIRT ADVIERTE DE MALWARE EN CORREO QUE SUPLANTA AL SII

Alerta de seguridad informática	2CMV-00040-001
Clase de alerta	Fraude
Tipo de incidente	Phishing - Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre de 2019

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing con malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Interno.

Los cibercriminales buscan engañar a los usuarios informando que este correo fue generado por un proceso de emisión de factura electrónica detectada el año 2018. A la potencial víctima, se le ofrece la posibilidad de descargar la factura electrónica desde un hipervínculo en el mismo correo. Al descargar el archivo y ser ejecutado, se desencadena la infección del malware.

Enlace

https://www.csirt.gob.cl/alertas/2cmv-00040-001/

https://www.csirt.gob.cl/media/2019/12/2CMV-00040-001.pdf

9VSA-00096-001 CSIRT COMPARTE ACTUALIZACIONES PARA FIREFOX Y FIREFOX ESR

Alerta de seguridad informática	9VSA-00096-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	5 de diciembre de 2019
Última revisión	5 de diciembre de 2019

Vulnerabilidad

CVE-2019-11745
CVE-2019-11756
CVE-2019-13722
CVE-2019-17005
CVE-2019-17008
CVE-2019-17009
CVE-2019-17010
CVE-2019-17011
CVE-2019-17012
CVE-2019-17013
CVE-2019-17014

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Mozilla referente a vulnerabilidades que afectan a Firefox y Firefox ESR, las cuales, de ser explotadas, pueden resultar en ataques de denegación de servicios, corrupción de datos y ejecución de código remoto, las que son consideradas como críticas. El informe incluye las respectivas actualizaciones para mitigar los riesgos asociados.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00096-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00096-001.pdf

9VSA-00097-001 CSIRT COMPARTE ACTAULIZACIONES DE VMWARE PARA ESXI Y HORIZON DAAS

Alerta de seguridad informática	9VSA-00097-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2019
Última revisión	6 de diciembre de 2019

Vulnerabilidad
CVE-2019-5544

Resumen
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de VMWare, referente a vulnerabilidades que afectan a sus productos ESXi y Horizon DaaS.

Enlace
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00097-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00097-001.pdf

9VSA-00098-001 CSIRT COMPARTE ACTUALIZACIONES PARA SISTEMA OPERATIVO DE ANDROID

Alerta de seguridad informática	9VSA-00098-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de diciembre de 2019
Última revisión	8 de diciembre de 2019

Vulnerabilidad
CVE-2019-2232
CVE-2019-9464
CVE-2019-2217
CVE-2019-2218
CVE-2019-2220
CVE-2019-2221
CVE-2019-2222
CVE-2019-2223
CVE-2019-2224
CVE-2019-2225
CVE-2019-2226
CVE-2019-2227
CVE-2019-2228
CVE-2019-2229
CVE-2019-2230
CVE-2019-2219
CVE-2019-2231
CVE-2018-20961
CVE-2019-15220
CVE-2019-15239
CVE-2019-10557
CVE-2018-11980
CVE-2019-10480
CVE-2019-10481
CVE-2019-10536
CVE-2019-10537

CVE-2019-10595
CVE-2019-10598
CVE-2019-10601
CVE-2019-10605
CVE-2019-10607
CVE-2019-2304
CVE-2019-2242
CVE-2019-10500
CVE-2019-10525
CVE-2019-10482
CVE-2019-10487
CVE-2019-10516
CVE-2019-2274
CVE-2019-10513
CVE-2019-10517
CVE-2019-10600

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Android, referente a vulnerabilidades que afectan su sistema operativo. De ser explotadas, estas pueden resultar en múltiples ataques, como exposición de información sensible, denegación de servicios permanente, ejecución de código remoto, entre otros. Junto a este informa se publican las respectivas actualizaciones para mitigar los riesgos.

Enlace

https://www.csirt.gob.cl/vulnerabilidades/9vsa-00098-001/
https://www.csirt.gob.cl/media/2019/12/9VSA-00098-001.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
5.189.172.74	Port Scan
113.188.161.147	Port Scan
5.251.252.252	Port Scan
207.180.193.223	Port Scan
45.76.64.121	Port Scan
219.250.188.185	Port Scan
1.53.167.127	Port Scan
54.36.124.145	Port Scan
158.181.147.136	Port Scan

167.86.68.12	Port Scan
181.40.66.205	Port Scan
185.164.72.69	Port Scan
189.137.5.250	Port Scan
2.99.108.252	Port Scan
185.164.72.60	Port Scan
37.139.30.95	Malware
14.242.178.212	Port Scan
178.124.153.97	Port Scan
1.1.229.152	Port Scan
178.27.185.94	Port Scan
45.176.240.44	Port Scan
167.86.115.114	Port Scan
77.247.109.41	Port Scan
103.248.220.89	Port Scan
188.159.119.6	Port Scan
2.152.28.203	Port Scan
216.151.184.184	Port Scan
116.240.199.86	Port Scan
46.38.144.202	Port Scan
167.86.115.113	Port Scan
114.35.75.217	Port Scan
200.7.124.69	Port Scan
59.26.114.155	Port Scan
199.231.115.146	Port Scan
196.221.12.78	Port Scan
185.153.197.161	Port Scan
103.85.18.99	Port Scan
167.172.220.39	Port Scan
91.187.80.246	Port Scan
108.191.2.72	Port Scan
188.152.7.140	Port Scan
114.183.140.94	Port Scan
172.105.213.30	Port Scan
107.161.88.35	Port Scan
199.195.252.32	Port Scan
80.82.70.106	Port Scan
89.248.162.161	Port Scan
80.82.70.106	Port Scan
89.248.162.161	Port Scan
185.119.42.212	Port Scan

71.6.142.85	Port Scan
51.75.165.119	Port Scan
163.172.8.221	Port Scan
176.31.131.255	Port Scan
37.49.231.100	Port Scan
45.95.168.103	Port Scan
104.131.96.177	Port Scan
27.254.63.38	Port Scan
197.156.100.198	Port Scan
197.133.103.199	Port Scan
167.86.79.146	Port Scan
176.107.133.144	Port Scan
41.140.245.116	Port Scan
186.66.12.10	Malware
190.195.129.227	Malware
149.202.153.251	Malware
79.172.249.82	Malware
37.132.193.19	Malware
200.123.101.90	Malware
172.104.233.225	Malware
104.236.137.72	Malware
38.68.36.182	Port Scan
213.232.126.18	Port Scan
54.39.161.175	Port Scan
217.61.20.216	Port Scan
203.148.85.146	Port Scan
171.226.227.237	Port Scan
185.234.219.85	Port Scan
113.160.11.178	Port Scan
27.78.26.29	Port Scan
115.23.68.239	Port Scan
92.47.194.254	Port Scan
212.124.126.82	Port Scan
185.200.118.35	Port Scan
159.203.170.238	Port Scan
167.99.126.92	Port Scan
14.190.43.162	Port Scan
104.219.234.53	Port Scan
217.12.200.200	Port Scan
103.4.166.242	Port Scan
145.239.150.181	Port Scan

207.38.90.13	Port Scan
77.247.110.16	Port Scan
115.201.99.116	Port Scan
124.16.131.251	Port Scan
220.184.186.51	Port Scan
115.217.18.73	Port Scan
123.96.130.4	Port Scan
125.104.219.143	DDoS
36.24.52.41	DDoS
115.201.100.72	DDoS
115.201.191.139	DDoS
115.201.137.93	DDoS
218.74.46.92	DDoS
218.71.148.62	DDoS
122.227.116.240	DDoS
36.24.54.107	DDoS
60.189.106.151	DDoS
36.24.44.221	DDoS
60.162.49.36	DDoS
183.144.5.240	DDoS
192.228.100.11	Port Scan
51.159.30.213	Port Scan
185.217.0.239	Port Scan
190.224.230.137	Port Scan
122.236.128.232	Port Scan
115.203.0.226	Port Scan
125.122.204.95	Port Scan
60.185.233.231	Port Scan
115.215.56.78	Port Scan
113.201.169.122	Port Scan
115.196.44.211	Port Scan
220.184.64.12	Port Scan
183.138.136.58	Port Scan
124.89.210.52	Port Scan
103.47.168.198	Port Scan
87.0.242.90	Port Scan
24.27.5.145	Port Scan
149.202.251.78	Port Scan
114.199.114.46	Port Scan
51.158.25.170	Port Scan
64.31.35.218	Port Scan

185.150.190.226	Port Scan
178.128.201.239	Port Scan
163.172.221.154	Port Scan
163.47.140.91	Port Scan
94.23.58.172	Port Scan
74.63.242.198	Port Scan
198.54.113.2	Port Scan
54.37.76.252	Port Scan
193.70.40.191	Port Scan
125.25.91.150	Port Scan
14.239.119.250	Port Scan
43.250.186.214	Port Scan
185.208.211.138	Port Scan
103.36.102.10	Port Scan
182.163.227.54	Port Scan
54.36.185.125	Port Scan
172.247.84.52	Port Scan
158.69.5.198	Port Scan
58.11.29.26	Port Scan
180.244.100.168	Port Scan
117.2.108.96	Port Scan
14.161.254.220	Port Scan
14.241.66.55	Port Scan
121.7.25.251	Port Scan
36.84.146.54	Port Scan
202.65.206.131	Port Scan
113.190.11.161	Port Scan
154.221.16.78	Port Scan
51.15.222.217	Port Scan
14.161.210.65	Port Scan
23.105.70.70	Port Scan
45.143.220.112	Port Scan
103.199.69.197	Port Scan
103.199.70.111	Port Scan
193.56.28.163	Port Scan
172.81.129.30	Port Scan
103.89.91.2	Port Scan
45.77.241.154	Port Scan
45.64.126.47	Port Scan
2.21.36.183	Port Scan
185.81.157.140	Port Scan

51.91.219.186	Port Scan
195.154.57.1	Port Scan
67.169.57.28	Port Scan
190.112.234.177	Port Scan
170.239.157.10	Port Scan
182.55.26.144	Port Scan
218.186.168.112	Port Scan
138.68.27.253	Port Scan
159.203.193.248	Port Scan
159.50.16.166	DDoS
142.93.245.188	Port Scan
89.174.201.133	Port Scan
93.48.65.53	Port Scan
92.138.35.0	Port Scan
45.87.167.22	Port Scan
213.183.62.133	Port Scan
104.131.176.211	Port Scan
37.120.149.150	Port Scan
192.99.216.181	Port Scan
152.32.191.35	Port Scan
129.232.219.209	Port Scan
103.18.56.58	Port Scan
185.123.101.128	Port Scan
37.143.130.124	Port Scan
211.22.158.74	Port Scan
139.162.189.5	Port Scan
155.94.254.7	Port Scan
172.104.97.121	Port Scan
172.105.40.217	Port Scan
192.40.57.232	Port Scan
23.108.65.85	Port Scan
62.210.89.203	Port Scan
45.143.221.27	Port Scan
45.134.179.240	Port Scan
5.188.168.41	Port Scan
36.90.19.143	Port Scan
177.66.247.170	Port Scan
104.200.134.160	Port Scan
190.109.203.229	Port Scan
51.75.153.29	Port Scan
138.68.218.135	Port Scan

62.210.89.189	Port Scan
77.247.109.46	Port Scan
77.247.108.90	Port Scan
212.129.23.154	Port Scan
179.43.149.24	Port Scan
51.91.158.49	Port Scan
47.56.25.28	Port Scan
147.135.121.66	Port Scan
212.129.55.255	Port Scan
183.82.102.113	Port Scan
192.95.62.169	Port Scan
220.117.90.7	Port Scan
27.75.22.105	Port Scan
192.95.62.175	Port Scan
58.161.152.103	Port Scan
88.218.195.130	Port Scan
185.103.110.186	Port Scan
193.29.15.234	Port Scan
185.53.88.18	Port Scan
47.75.181.99	Port Scan
165.16.127.245	Port Scan
118.193.28.58	Port Scan
110.137.103.133	Port Scan
103.8.118.112	Port Scan
79.156.253.240	Port Scan
119.252.174.146	Port Scan
77.247.109.40	Port Scan

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: 2019.12.14 13:52:07 -03'00'