CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Reporte sobre ataques cibernéticos entre los días 21 y 25 de octubre de 2019.

Santiago, 28 de Octubre del 2019

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Nota

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. **La información contenida en los informes o comunicados está afecta a actualizaciones.**
Este informe ha sido clasificado con TLP BLANCO. La información puede ser distribuida sin restricciones.

Resumen Ejecutivo

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectó tráfico anómalo en la red de conectividad del Estado y en los sitios web de gobierno y otros sitios públicos que visualiza a través de sus plataformas. Esta anomalía fue detectada entre los días lunes 21 y viernes 25 de octubre de 2019.

El siguiente documento resume los eventos y ataques ocurridos durante esos días. CSIRT pudo identificar diferentes fuentes de ataques, siendo la gran mayoría internacionales, y otros nacionales.

Cronología de Eventos

1. **Modificación no autorizada de información en página de pagos de la Municipalidad de Macul**

Lunes 21
09:00 horas

CSIRT fue advertido de una vulnerabilidad explotada en una página web del sitio oficial de la Municipalidad de Macul. El sitio fue vulnerado en dos ocasiones. En ambos ataques fueron publicadas consignas políticas.

Si bien la URL es parte del sitio, ésta no se encuentra referenciada directamente en el sitio. No obstante, si se podía acceder digitando la URL, lo que limitaba su visibilidad hacia el público.

CSIRT reportó lo ocurrido en ambas oportunidades, asociadas al ticket #2019102157000961.

El problema se encuentra superado. CSIRT está en conocimiento que se está migrando la plataforma a una más actualizada y robusta en seguridad.

Resultado: Hubo afectación, Defacement.

2. **Ataques de DDOS generalizados contra redes del Estado**

Lunes 21 y Martes 22
Todo el día

Se produjeron dos ataques de denegación de servicios, los que buscaban paralizar los sistemas informáticos del gobierno. El primer ataque se registró entre la tarde del domingo 20 y la madrugada del lunes 21 de octubre. El segundo ataque, acaeció entre la noche del 21 hasta la madrugada del 22 de octubre. Los siguientes, son los indicadores de compromisos asociados al ataque.

Indicadores de compromiso:

IP
194.187.175.68
69.162.126.126
37.49.231.156
159.203.201.41
62.234.92.113

198.108.67.96
78.157.209.34
185.39.11.41
89.248.160.178
185.176.27.94
185.175.93.18
77.40.4.202
51.89.125.75
191.114.52.29
80.211.244.140
104.192.0.62
159.203.201.38
13.59.252.119
139.162.235.92
200.28.77.151
201.189.20.253
200.28.89.224
181.203.59.74
186.104.70.200
181.163.50.170
179.8.102.80
186.106.58.211
129.78.110.128
139.19.117.8
198.108.67.112
198.12.64.90
190.5.48.132
51.38.67.162
133.34.149.5
185.40.13.3
31.166.40.210
82.196.5.139
194.187.175.68
187.189.155.205
217.61.59.165
172.58.235.123
201.219.175.159
152.231.32.212
178.148.27.26
179.7.225.94
186.84.193.159
64.59.96.67
157.37.196.149
189.217.25.216
186.120.90.2
200.86.190.183

190.20.144.6
179.8.55.186
190.37.217.223
181.46.136.142
189.186.234.207
186.51.195.107
185.176.27.114
141.168.65.80
181.115.30.153
191.88.96.17
186.111.153.74
186.84.90.190
190.159.208.199
181.129.217.34
80.211.240.4
77.247.110.73
172.105.26.90
172.105.215.250
50.116.42.192
74.207.231.72
69.171.251.134
173.212.248.207
190.92.0.5
138.246.253.21
66.220.156.50
66.220.156.53
192.236.194.154
88.198.139.2
185.40.13.3
222.187.200.229
89.248.169.12
134.209.173.240
190.164.53.171
190.196.60.169
193.201.28.35
194.187.175.68
190.8.119.74
200.28.77.151
201.189.20.253
200.28.89.224
181.203.59.74
186.104.70.200
181.163.50.170
179.8.102.80
186.106.58.211
159.203.201.96

80.82.48.104
45.136.109.48
159.89.34.120
23.247.118.11
80.82.65.74
77.247.110.162
144.91.76.173
212.60.5.8
92.118.37.70
159.89.34.120
158.69.58.33
186.20.255.188
138.68.0.180
131.255.7.87
185.216.140.252
186.104.157.97
200.83.20.159
190.47.167.118
80.82.78.104
186.104.131.12
200.27.2.65
205.185.124.24
200.83.18.42
68.183.16.183
196.240.255.14
51.38.107.66
66.220.151.250
66.220.151.252
119.225.142.246
45.131.68.37
190.160.0.51
94.142.136.100
129.28.29.30
144.217.7.33
158.69.58.33
179.4.213.97
203.80.136.133
204.12.240.85
159.203.192.250
81.22.45.170
92.118.37.88
185.136.204.36
185.136.204.35
23.228.101.195
185.140.55.94
67.211.209.151

159.203.201.80
144.91.76.173
45.143.221.2
191.115.95.26
201.189.30.172
191.126.99.170
191.115.5.137
191.125.139.13
191.125.139.13
190.22.0.122
186.104.146.24
190.21.123.27
190.21.104.223
190.153.227.203
45.76.0.183
176.32.34.88
172.105.69.121
89.248.178.217
95.217.255.76
173.252.99.240
173.252.92.120
45.119.240.78
200.11.176.52
207.246.84.11

Resultado: No hubo afectación.

3. Ataque DDOS a Ministerio de Agricultura

Martes 22
02:30 horas

CSIRT detectó una notoria alza de conexiones hacia una IP del Ministerio de Agricultura lo que fue oportunamente reportado a la institución y quedó consignado en el ticket # 2019102257000209 a las 02:43 horas.

A partir de eso momento CSIRT bloqueo las IP's que se indican a continuación, repeliendo el ataque.

A continuación se listan los indicadores de compromiso asociados al ataque.

IP Origen:
34.201.223.181

Resultado: No hubo afectación.

4. **Incidente de intrusión, compromiso de cuenta privilegiada en canal de TV MEGA**

Martes 22 de Octubre
15:00 horas

CSIRT, fue advertido de la publicación en el repositorio pastebin de información correspondiente a IPs públicas de servidores de la estación de televisión MEGA.

A las 16:32 horas, CSIRT abrió el ticket #2019102257000791 y se contactó con la estación de televisión, recomendando al canal privado tomar precauciones para evitar un incidente dirigido a su servicio de streaming.

Resultado: No hubo afectación.

5. **Ataque contra el Ministerio de Agricultura**

Martes 22
Durante el día

CSIRT detectó una notoria alza de conexiones en dirección al Ministerio de Agricultura. Este ataque fue repelido.

Resultado: No hubo afectación.

6. **Ataque de DDOS contra Ministerio del Interior y Seguridad Pública**

Miércoles 23
00:07 horas

CSIRT detecta ataque de denegación de servicios y se procede a abrir el ticket #Ticket2019102357000029. Se registra la IP de origen como la:

190.5.48.132

Se procedió a bloquear la IP y reportar a la institución.

Resultado: No hubo afectación.

7. **Ataque contra el Ministerio de Vivienda y Urbanismo**

Miércoles 23
18:20 horas

CSIRT detectó un ataque de DDOS que generó múltiples conexiones hacia el Ministerio de Vivienda y Urbanismo. Quedó consignado en el #Ticket2019102357000565. Las IP asociadas fueron:

190.163.175.80
190.45.244.242

Ambas fueron bloqueadas oportunamente y reportada a la institución

Resultado: No hubo afectación.

8. **Filtración de datos Ministerio del Interior**

Miércoles 23
20:30 horas

CSIRT fue advertido por una fuente del Estado sobre una filtración de bases de datos que fueron expuestas en internet y que contenían usuarios y contraseñas de correos electrónicos del Ministerio del Interior.

Resultado: No hubo afectación.

9. **Filtración de datos Banco Central**

Miércoles 23
22:30 horas

CSIRT advirtió de la publicación de una base de datos del Banco Central. CSIRT procedió a abrir el ticket t#2019102257000905. La información fue contrastada con fuentes del propio banco, las que durante la misma noche confirmaron que la base de datos era antigua, que las cuentas estaban desactivadas, y que ellos estaban en conocimiento de esta información hace mucho tiempo atrás.

Resultado: No hubo afectación.

10. **Ataque contra el Ministerio del Interior**

Jueves 24
00:10 horas

CSIRT detectó un ataque de DDOS dirigido al Ministerio del Interior y Seguridad Pública. Las IP involucradas fueron:

188.165.219.27

198.50.183.35

Ambas IP fueron bloqueadas oportunamente y reportadas a la institución.

Resultado: No hubo afectación.

11. Suplantación de sitio web elige vivir sin drogas

Jueves 24
01:23 horas

CSIRT detecta la suplantación del sitio elige vivir sin drogas. Se procede a abrir el ticket 2019102457000143. CSIRT reportó al Hosting ibb.co, en el cual se aloja este sitio web que simula ser del Gobierno de Chile, para que procediera a bajarlo, lo que se logó con éxito al cabo de unos minutos.

Resultado: No hubo afectación.

12. Ataque DDOS contra Junaeb

Jueves 24
04:20 horas

Fue detectado un ataque de DDOS contra el sitio de Junaeb. De acuerdo al ticket 2019102457000321 abierto por CSIRT, la IP bloqueada fue:

138.99.224.159

La información fue reportada oportunamente a la institución.

Resultado: No hubo afectación

13. Defacement Municipalidad de San Nicolás

Jueves 24
06:09 horas

CSIRT fue informado de un defacement en una página del sitio web de la Municipalidad de San Nicolás. Se procedió a la apertura del ticket 2019102457000376.

CSIRT informó oportunamente a la institución y se logró mitigar el ataque.

Resultado: Hubo afectación

14. Ataques contra el Ministerio de Vivienda

Se detectan dos ataques de DDOS contra el Ministerio de Vivienda y Urbanismo. Ambos ataques fueron repelidos.

El primero de los ataques ocurrió a las 18:25 horas. El segundo a las 20:55 horas.

Los Índices de Compromiso asociados son:
177.67.82.218
177.67.82.210

Resultado: no hubo afectación

15. Sabotaje informático en servicios de transportes de Santiago

Toda la semana

CSIRT advirtió de ataques y amenazas a los sistemas informáticos y sitios web del transporte urbano de Santiago, y a las operaciones de algunos servicios privados que realizan conexión con el Aeropuerto Internacional de la capital.

CSIRT se contactó con algunos de los afectados por el sabotaje, para advertir del suceso y ofrecer colaboración para la mitigación temporal de las vulnerabilidades, las que se dan en el contexto de ataques a otras entidades vinculadas a los transportes como METRO (19 de octubre) y DTPM (20 de octubre).

Resultado: Hubo afectación.

16. Ataque contra el Ministerio de Justicia

Viernes 25
03:45 horas

Se detecta que un ataque de denegación de servicios hacia el Ministerio de Justicia. El ataque fue repelido. Se procedió a la apertura del ticket 019102557000557

17. Filtración de base de datos de Carabineros de Chile

Viernes 25
16:20

CSIRT advirtió de la filtración de la base de datos de 29.952 mil funcionarios de Carabineros de Chile. La información fue hecha pública en una cuenta de twitter. CSIRT procedió a

contactarse con la institución, la que más tarde confirmó que se trataba de una base de datos oficial.

La base de datos se encontraba en diferentes sitios e incluye el nombre, correo, zona, prefectura y comisaría de pertenencia y otros antecedentes.

La institución tomó medidas, entre ellas, la cancelación del servicio de correos internos.

Resultado: hubo afectación.

18. Defacement página del sitio del SENAME

Viernes 25
16:25 horas

CSIRT advierte de defacement en una página del sitio de SENAME. CSIRT se contacta con los administradores del sitio. A las 17:00 horas el sitio deja de estar activo para subsanar el problema.

Resultado: hubo afectación

19. Ataque de DDOS hacia el Ministerio de Economía

Viernes 25
19:00 horas

CSIRT detectó un ataque de DDOS que generó múltiples conexiones hacia el Ministerio de Economía. La IP asociada al ataque fue bloqueada e identificada:

35.239.45.46

Resultado: No hubo afectación del servicio

20. Amenaza y ataque contra Radio BioBío

Viernes 25
20:25 horas

CSIRT fue advertido por terceros de amenazas de ataques contra la radioemisora BioBío. Se busca contactó en la entidad para que tomaran precauciones. La entidad sufrió una breve interrupción en su sitio web producto de ataque DDOS cerca de las 22:30 horas, situación que fue subsanada.

Resultado: hubo afectación

21. Ataque contra sitio del Senado de la República

Viernes 25
23:00 horas

Se registra la caída del sitio del Senado de la República producto de un ataque de DDOS. CSIRT tomó contacto con la entidad para informar. El sitio tuve una breve interrupción, la que fue rápidamente subsanada para luego seguir funcionando con normalidad.

Resultado: hubo afectación

22. Ataque contra MOP y DGA

Viernes 25
23:00 horas

Se registra ataque DDOS contra el Ministerio de Obras Públicas y la Dirección General de Aguas. La entidad informó del ataque y se comienzan a tomar medidas de mitigación. Ambos sitios fueron declarados en mantención como medida preventiva y se bloquean IP's.

Resultado: no hubo afectación

23. Otros índices de compromiso asociados al informe

IoC	Motivo
190.5.48.132	DDoS
164.132.7.22	Port Scan
171.67.70.128	Port Scan
36.84.184.242	Port Scan
104.237.227.211	Port Scan
190.163.33.49	Port Scan
148.251.94.74	Port Scan
1,90141E+11	Port Scan
67.242.131.15	Port Scan
50.63.14.162	Port Scan
103.81.86.125	Port Scan
185.245.86.69	Port Scan
69.175.59.186	Port Scan
177.247.65.226	Port Scan
45.79.55.196	Port Scan
185.175.93.25	Port Scan
173.212.214.68	Port Scan
45.136.110.49	Port Scan

159.203.20.1164	Port Scan
194.187.172.9	Port Scan
51.38.67.162	Port Scan
195.154.189.15	Port Scan
185.153.197.237	Port Scan
159.203.201.94	Port Scan
159.203.201.85	Port Scan
190.2.141.250	Port Scan
92.63.194.70	Port Scan
92.63.194.30	Port Scan
103.59.166.8	Port Scan
112.175.124.2	Port Scan
112.175.127.189	Port Scan
190.163.175.80	DDoS
190.45.244.242	DDoS
185.153.199.14	Port Scan
45.33.48.143	Port Scan
45.33.59.87	Port Scan
45.33.49.87	Port Scan
195.154.32.212	Port Scan
112.175.127.186	Port Scan
177.232.85.234	Port Scan
45.103.220.21	Port Scan
64.71.187.44	Port Scan
51.89.251.196	Port Scan
77.247.108.125	Port Scan
112.175.126.18	Port Scan
198.50.183.35	DDoS
188.165.219.27	DDoS
162.244.80.38	Port Scan
37.49.227.109	Port Scan
159.203.201.239	Port Scan
31.13.114.124	Port Scan
185.172.110.222	Port Scan
37.49.227.109	Port Scan
190.47.113.147	Port Scan
138.99.224.159	DDoS
167.86.71.238	Port Scan
144.91.76.115	Port Scan
176.107.133.164	Port Scan
144.91.76.115	Port Scan
45.143.220.21	Port Scan
138.201.232.60	Port Scan
172.105.25.41	Hacking
211.44.226.158	Port Scan

112.175.127.179	Port Scan
112.175.124.2	Port Scan
217.182.196.164	Port Scan
62.210.177.9	Port Scan
51.15.27.103	Port Scan
177.67.82.218	DDoS
177.67.82.210	DDoS
89.248.169.17	Port Scan
194.99.104.35	Port Scan
37.49.231.123	Port Scan
162.244.80.228	Port Scan
198.74.53.233	Port Scan
185.53.88.72	Port Scan
159.203.193.41	Port Scan
49.45.28.6	Port Scan
193.201.224.199	Port Scan
172.105.151.161	Port Scan
89.248.174.206	Port Scan
188.240.220.58	Port Scan
92.118.37.95	Port Scan
173.44.55.155	DDoS
185.209.0.31	Port Scan
185.209.0.58	Port Scan
88.208.3.143	Port Scan
185.209.0.83	Port Scan
77.247.108.119	Port Scan
83.97.20.47	Port Scan
31.184.218.239	Port Scan
95.213.242.138	Port Scan
159.203.201.236	Port Scan
5.254.74.2	Port Scan