CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Cyber Attacks between October 21-25, 2019.

Santiago, October 26, 2019

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Note

The information contained in this report is the product of the analysis of multiple sources, third parties and research of the CSIRT team. The information contained in the reports or releases is affecting updates.
This report has been classified with TLP WHITE. The information can be distributed without restrictions.

Summary

The Computer Security Incident Response Team, CSIRT, detected anomalous traffic on the state connectivity network and on government websites and other public sites that it visualizes through its platforms. This anomaly was detected between Monday 21 and Friday 25 October 2019.

The following document summarizes the events and attacks that occurred during those days.

Incidents record

1. **Unauthorized modification, payment website of the Municipality of Macul**

Monday 21
09:00 hours

CSIRT was warned of a vulnerability exploited on the official website of the Municipality of Macul. Political slogans were published.

The problem was resolved. CSIRT is aware that the platform is being migrated to a more updated and robust security.

Result: There was affectation, Defacement.

2. **Generalized DDOS attacks against state networks**

Monday 21, Tuesday 22
All day

There were two denial of service attacks, which sought to paralyze government computer systems. The first attack was recorded between the afternoon of Sunday 20 and the morning of Monday, October 21. The second attack occurred between the night of 21 until the dawn of October 22. The following are the IoCs associated with the attack.

IoC
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

Result: There was no involvement.

3. DDOS attack on the Ministry of Agriculture

Tuesday 22
02:30 hours

CSIRT detected an increase of connections to the Ministry of Agriculture server which was duly reported to the institution and was recorded on ticket # 2019102257000209 at 02:43 hours.

From that moment on, CSIRT blocked the IPs indicated below, repelling the attack.

Source IP:

34,201,223,181

Result: There was no involvement.

4. Intrusion incident, privileged account commitment on MEGA TV channel

Tuesday 22 October
3:00 p.m.

CSIRT was warned of a pastebin publication that contained MEGA TV public IPs.

At 4:32 p.m., CSIRT opened the ticket # 2019102257000791 and contacted the television station, recommending that MEGA should take precautions to avoid an incident aimed at its streaming service.

Result: There was no involvement.

5. **Attack on the Ministry of Agriculture**

Tuesday 22
All day

CSIRT detected a noticeable rise in connections to the Ministry of Agriculture. This attack was repelled.

Result: There was no involvement.

6. **DDOS attack against the Ministry of Interior and Public Security**

Wednesday 23
00:07 hours

CSIRT detects denial of service attack and proceeds to open ticket # Ticket2019102357000029. The source IP is registered as:

190.5.48.132

The IP was blocked and reported to the institution.

Result: There was no involvement.

7. **Attack on the Ministry of Housing and Urban Planning**

Wednesday 23
18:20 hours

CSIRT detected a DDOS attack against the Ministry of Housing and Urban Planning. It was listed in # Ticket2019102357000565. The associated IPs were:

190,163,175.80
190.45.244.242

Both were timely blocked and reported to the institution.

8. **Ministry of Interior filtered data**

Wednesday 23
20:30 hours

CSIRT was warned by a source of the State about a leak of databases that were exposed on the Internet that contained users and passwords of emails from the Ministry of Interior.

Result: There was no involvement.

9. Central Bank filtered data

Wednesday 23
10:30 p.m.

CSIRT warned to the Central Bank about a database exposure. CSIRT proceeded to open the ticket # 2019102257000905. The information was contrasted with sources from the bank itself, which on the same night confirmed that the database was old, that the accounts were deactivated, and that they were aware of this information long ago.

Result: There was no involvement.

10. Attack on the Interior Ministry

Thursday 24
00:10 hours

CSIRT detected a DDOS attack against the Ministry of Interior and Public Security. The IPs involved were:

188,165,219.27
198.50.183.35

Both IPs were blocked in a timely manner and reported to the institution.

Result: There was no involvement.

11. Fraudulent website of the "live without drugs" program

Thursday 24
01:23 hours

CSIRT detected a cloned paged called “Live Without Drugs” that is a copy of a governmental campaign. The ticket #2019102457000143 is opened. CSIRT reported to the ibb.co Hosting, where this website that pretends to be from the Chilean Government is hosted, so it could be shut down, which was successfully achieved after a few minutes.

Result: There was no involvement.

12. DDOS attack on Junaeb

Thursday 24
04:20 hours

A DDOS attack was detected against the Junaeb site. According to the ticket #2019102457000321 opened by CSIRT, the blocked IP was:

138.99.224.159

The information was timely reported to the institution.

Result: There was no affectation

13. Defacement, Municipality of San Nicolás

Thursday 24
06:09 hours

CSIRT was informed of a defacement on the page of Municipality of San Nicolás. The ticket #2019102457000376 was opened.

CSIRT informed the institution in a timely manner and the attack was mitigated.

Result: There was affectation

14. Attacks against the Ministry of Housing

Two DDOS attacks are detected against the Ministry of Housing and Urban Planning. Both attacks were repelled.

The first of the attacks occurred at 6:25 p.m. The second at 8:55 p.m.

The associated IoCs are:
177.67.82.218
177.67.82.210

Result: there was no affectation

15. Computer sabotage in transport services of Santiago

All week

CSIRT warned of attacks and threats to the computer systems and urban transport websites of Santiago, and to the operations of some private services that connect with the International Airport of the capital.

CSIRT contacted some of those affected by sabotage, to warn of the event and offer collaboration for the temporary mitigation of vulnerabilities, which occur in the context of attacks on other entities linked to transport such as METRO (October 19) and DTPM (October 20).

Result: There was involvement.

16. Attack on the Ministry of Justice

Friday 25
03:45 hours

It is detected that a denial of service attack towards the Ministry of Justice. The attack was repelled. The ticket was opened #019102557000557

17. Database dump, Carabineros de Chile

Friday 25
16:20

CSIRT warns of the filtration of the database of 29,952 thousand officials of Carabineros de Chile. The information was made public on a twitter account. CSIRT proceeded to contact the institution, which later confirmed that it was an official database.

The database was in different places and includes the name, mail, area, prefecture and police station of membership and other background.

The institution took measures, including the cancellation of the internal mail service.

Result: there was involvement.

18. Defacement SENAME website

Friday 25
4:25 p.m.

CSIRT warns of defacement on a page of the SENAME site. CSIRT contacts the site administrators. At 5:00 p.m., the site is no longer active.
Result: there was involvement

19. DDOS attack on the Ministry of Economy

Friday 25
7:00 p.m.

CSIRT detected a DDOS attack to the Ministry of Economy. The IP associated with the attack was blocked and identified:

35.239.45.46

Result: There was no affectation of the service

20. Threat and attack against Radio BioBío

Friday 25
20:25 hours

CSIRT gathers information about threat of denial of service attack against the BioBío radio station. The entity suffered a brief interruption on its website due to DDOS attack at about 10:30 pm, a situation that was corrected.

Result: there was involvement

21. Attack on the site of the Senate of the Republic

Friday 25
23:00 hours

They received a DDoS attack. CSIRT contacted the entity to inform. The site remained down for about 5 minutes, and then continued to function normally.
Result: there was affectation

22. Attack against MOP and General Water Directorate

Friday 25
23:00 hours

DDOS attack is registered against the Ministry of Public Works and the General Water Directorate. The entity reported the attack and mitigation measures began. Both sites were declared in maintenance as a preventive measure and IP's were blocked.

Result: there was no affectation

23. IoCs

IoC	Motive
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