CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Reporte sobre ataques cibernéticos durante el fin de semana entre el 19 y 20 de octubre de 2019.

Santiago, 21 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 que visualiza a través de sus plataformas. Esta anomalía fue detectada entre los días sábado 19, domingo 20 y lunes 21 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. En este último caso, CSIRT pudo confirmar que existió concertación por parte de grupos nacionales para la perpetración de actividad maliciosa.

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno
de Chile
Fecha: 2019.10.21
20:55:42 -03'00'

Cronología del Caso

1. **Supuesta exposición de base de datos de funcionarios de Metro de Santiago**

El día sábado 19 de octubre, a las 12:13 horas, CSIRT tuvo antecedentes sobre la publicación de una base de datos filtrados de usuarios de la empresa METRO. CSIRT procedió a informar de la situación a la empresa a través del ticket #2019101957000288 emitido a las 12:31 horas.

La empresa revisó la base de datos para validar las cuentas adjuntadas por CSIRT. Paralelamente, CSIRT verificó si las cuentas eran válidas. Ambas instituciones descartaron la información publicada, la que si bien eran institucionales, estas estaban desactivadas.

Debido a que la información fue publicada vía redes sociales, en el repositorio pastebin y a través de portales web nacionales, CSIRT procedió a emitir un desmentido vía twitter.

Resultado: La información era falsa. No hubo afectación.

2. **Ataque DDOS a JUNAEB**

El sábado 19 de octubre, a las 12:20 horas se detectó la caída del sitio oficial de la Junta Nacional de Auxilio Escolar y Becas (https://www.junaeb.cl), el que se encuentra alojado fuera de la Red de Conectividad del Estado y sin denominación *gob.cl

CSIRT concluyó que la caída del sitio web fue producto de un ataque de denegación de servicios (DDOS).

CSIRT procedió a informar de lo acontecido a la institución a través del ticket #2019101957000313 emitido a las 13:18 horas.

En paralelo, CSIRT procedió al bloqueo preventivo de las IP's maliciosas que pudieran afectar a la RCE.

Indicadores de compromiso

IP Origen:

66.249.85.10
66.249.85.12
66.249.85.13
181.161.179.48

Resultado: Si hubo afectación.

3. Ataque DDOS a MINEDUC

El sábado 19 de octubre, cerca de las 16:40 horas, CSIRT detectó en su monitoreo un tráfico anómalo y un alza notoria en las conexiones con destino a MINEDUC (Ministerio de Educación) lo que fue oportunamente reportado a la institución y que quedó consignado en el ticket #2019101957000359 a las 17:26 horas.

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

Indicadores de compromiso

IP Origen:

201.188.24.214
152.174.89.190
191.110.182.186
138.99.224.170
186.11.96.124
191.119.68.147
186.34.7.97
186.11.37.137
191.119.156.42
190.101.236.226

Resultado: No hubo afectación.

4. Ataque DDOS a Gobierno Digital

El domingo 20 de octubre, a las 15:57 horas, CSIRT detectó alertas en monitoreo de sitios web asociados al dominio gob.cl, lo que se tradujo en 3 minutos de indisponibilidad. Los dominios se recuperaron a las 15:59 horas, debido a la oportuna acción de Gobierno Digital.

CSIRT se puso en contacto telefónicamente con los responsables de los servicios afectados para prestar apoyo, el que no fue necesario debido a la rápida acción de la entidad.

Resultado: Hubo afectación. Indisponibilidad del servicio durante 3 minutos.

5. DDOS generalizados contra redes del Estado

Desde la tarde del domingo 20 hasta la madrugada del lunes 21, CSIRT identificó una serie de ataques de DDOS contra la Red de Conectividad del Estado, las que fueron repelidas.

Indicadores de compromiso:

IP's Involucradas:
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
144.91.76.173
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

Modificación no autorizada de información en contra DTPM

Durante el domingo CSIRT confirmó la información que circulaba por medios de comunicación y que hacía referencia a que el sitio web de la Dirección de Transporte Público Metropolitano, el que se encuentra alojada fuera de la Red de Conectividad del Estado, el que fue vulnerado e intervenido por terceros.

CSIRT reportó lo ocurrido oficialmente a las 19:55 horas con el ticket #2019102057000678.

A las 20:22 horas, la entidad pública fue informada de la situación.

Mientras se subsana el problema, el sitio web redirige a los usuarios a la dirección http://www.interior.gob.cl.