Alerta de seguridad informática	**2CMV-00031-001**
Clase de alerta	**Código Malicioso**
Tipo de incidente	**Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**05 de Septiembre de 2019**
Última revisión	**05 de Septiembre de 2019**

NOTIFICACIÓN

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, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, detectado un nuevo script malicioso que se encuentra activo. El malware tiene relación con el Informe sobre actividad maliciosa dirigida contra la ciudadanía y el sistema financiero nacional vía uso proxy change y extensión de Chrome publicado por el CSIRT de Gobierno recientemente.[1]

Este malware realiza dos acciones maliciosas. La primera, a través de una extensión de Google Chrome que al ser instalada redirige a los usuarios a sitios bancarios fraudulentos. La segunda acción realiza una configuración en las opciones de proxy del sistema operativo para los mismos fines.

Los usuarios se exponen a ser víctimas del robo de sus credenciales bancarias por la navegación en un sitio bancario fraudulento.

En el informe indicado anteriormente fueron identificados 1.121 hosts infectados. Con los nuevos hallazgos que se han realizado fueron identificados otros 373 host. Este nuevo script tiene el mismo *modus operandi* pero se diferencia por la complejidad en la técnica de ofuscación.

[1] La información está disponible en el sitio http://www.csirt.gob.cl en la sección reportes. El documento identificado como 10CND-00017-001 fue publicado el 4 de septiembre de 2019.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

https[:]//bbva[.]bancocl[.]com
https[:]//falabella[.]bancocl[.]com
https[:]//bice[.]bancocl[.]com
https[:]//bci[.]bancocl[.]com
https[:]//santander[.]bancocl[.]com
https[:]//officebanking[.]bancocl[.]com
https[:]//chile[.]bancocl[.]com
https[:]//scotiabankchile[.]bancocl[.]com
https[:]//scotiabankchile[.]bancocl[.]com
https[:]//estado[.]bancocl[.]com
https[:]//itau[.]bancocl[.]com
https[:]//ripley[.]bancocl[.]com
https[:]//security[.]bancocl[.]com

http[:]//www[.]thenewworking[.]info
http[:]//novocontador[.]club/mvk/controller[.]php
http[:]//novocontador[.]club/mvk/index[.]php
http[:]//novocontador[.]club/eco

IP

144[.]208[.]127[.]212
176[.]31[.]60[.]248
217[.]195[.]153[.]117

IOC

Name: mvkcl.dat
SHA256: C40621A0FCF81FF5535546C8C728456BE77A114D13BAB47937413C4A15C55556

Name: chrome.zip
SHA256: 2140C171B755A56A05CFE4A953579383592910B2A634B08E091F14254BF16CE4

Name: chrome.ico
SHA256: A4507FF4BC28F568F29B869C3879F0C89D034DE6488890C1AA98DE543A258BC2

Name: chrome.js
SHA256: 4E29B5BB3FF3940630BB277621BBDAC81FE88C0886D53586E9679662C60180EB

Name: manifest.json
SHA256: 5702541B7245B28BB75EBFA036DF694ED366136446C110F2DDDED2F1E1DEC522

Name: NHXs6bAW.txt (JS)
SHA256: 90326B06DC9C1CD05199ABAC573FA09BCBBDF463609133C81C88F22F6F6108C2

Name: chrome.zip
SHA256: E15E60BEDC7339CF3EEC372D2BEE61FC161C7E36BA451CE4E9C86FB782B4290C

Name: chrome.js
SHA256: 1D066A44012B6D3A29A5B6421B07846AA9B7C9623298910C4F339660B3589F1A

Name: manifest.json
SHA256: 0F12CF6BD4115153A9E4F6BB2C28E9BC35EDABCAE59DA729CAB34EFA03052149

Name: d.dat
SHA256: SHA25622ac00495b51044e792ec3376d6e280e9522feac471a00638d8fdbc90d4ce2da

IP's afectadas por el Malware

Estas IP's no son indicadores de compromisos para ser bloqueadas, sino para mostrar la magnitud del ataque. Tener en consideración que estas IP son asignaciones temporales dispuestas por el proveedor de internet en forma dinámica, en un espacio y tiempo dado, lo cual pudo corresponder al momento de la infección.

138.186.121.143	190.121.116.100	191.126.180.174	181.72.36.165	190.45.160.54	200.104.4.148
152.172.223.111	190.160.142.230	191.126.180.211	181.72.44.29	190.45.226.74	200.104.46.157
152.231.104.234	190.160.146.225	200.104.153.117	181.72.47.96	190.45.253.5	200.104.91.223
168.196.201.108	190.160.162.248	200.104.169.129	181.72.59.2	190.45.254.221	200.120.1.50
168.196.201.134	190.161.176.254	200.104.216.154	181.73.142.151	190.45.83.6	200.120.73.23
168.196.202.251	190.161.206.104	201.188.156.201	181.73.15.103	190.46.103.104	200.120.89.249
168.196.203.124	190.162.121.142	201.189.131.117	181.73.26.145	190.46.134.179	200.126.37.196
170.239.189.171	190.162.170.199	201.189.138.122	181.73.78.46	190.46.15.235	200.28.141.40
181.162.135.127	190.162.248.148	201.189.232.202	181.74.190.111	190.46.172.215	200.28.159.45
181.163.217.220	190.163.113.103	201.214.163.117	181.75.18.10	190.46.210.241	200.41.94.110
181.203.109.187	190.163.140.179	201.214.248.157	186.10.186.10	190.46.64.40	200.50.106.110
186.103.154.102	190.163.147.161	201.215.101.193	186.10.186.4	190.47.134.232	200.54.223.186
186.103.179.196	190.163.213.222	201.215.114.160	186.10.214.49	190.47.181.144	200.54.77.62
186.106.135.112	190.163.246.116	201.215.145.158	186.10.216.127	190.47.187.82	200.72.13.227
186.156.180.251	190.164.240.177	201.215.171.103	186.10.225.81	190.47.84.3	200.72.241.35
186.156.211.112	190.196.113.157	201.215.172.208	186.10.252.218	190.47.92.162	200.74.43.214
186.156.225.187	190.208.171.225	201.219.233.127	186.103.155.99	190.5.32.21	200.75.11.165
190.100.216.214	190.211.161.110	201.219.233.180	186.103.159.65	190.5.32.36	200.83.112.90
190.100.248.157	190.216.144.139	201.220.104.193	186.104.59.101	190.5.32.47	200.83.159.219
190.101.149.233	190.217.148.150	201.223.162.203	186.106.248.69	190.5.32.87	200.83.2.4
190.101.151.184	190.217.196.129	201.223.213.134	186.106.89.87	190.5.32.93	200.83.236.175
190.101.249.195	191.116.145.138	201.239.156.252	186.107.90.122	190.5.48.15	200.83.51.146
190.102.251.152	191.116.151.138	201.241.162.113	186.11.0.254	190.5.48.17	200.85.217.184

190.102.251.181	191.119.119.155	201.241.244.107	186.11.1.154	190.5.48.186	200.86.110.86
190.102.251.251	191.119.172.170	201.246.163.209	186.11.103.118	190.5.48.226	200.86.123.84
190.107.226.243	191.125.140.143	201.246.253.171	186.11.11.124	190.5.48.252	200.86.141.182
190.107.226.249	191.125.156.109	201.246.255.189	186.11.16.43	190.5.48.48	200.86.155.26
190.107.228.158	191.126.135.195	138.99.224.133	186.11.22.9	190.5.48.73	200.86.92.21
138.99.224.194	179.4.118.209	179.9.162.211	186.11.25.108	190.5.54.83	200.89.44.116
138.99.224.36	179.4.144.47	179.9.17.210	186.11.26.78	190.54.22.2	200.89.52.70
138.99.224.53	179.56.110.238	179.9.70.137	186.11.53.68	190.8.107.156	201.188.18.198
143.208.55.158	179.56.187.61	179.9.78.52	186.11.66.163	190.82.114.238	201.188.48.231
143.255.105.5	179.56.254.197	181.160.12.73	186.11.67.138	190.82.132.119	201.188.69.97
143.255.106.19	179.56.30.90	181.160.32.54	186.11.69.84	190.95.122.88	201.189.232.22
152.172.204.68	179.57.139.239	181.161.18.64	186.11.84.186	190.95.48.158	201.189.95.220
152.174.39.70	179.8.34.208	181.161.2.249	186.11.84.58	190.96.71.19	201.214.227.28
152.231.116.98	179.9.111.245	181.161.23.63	186.11.86.201	190.96.84.106	201.215.10.117
170.245.50.155	181.162.19.167	181.161.4.140	186.11.87.190	190.98.215.27	201.215.134.24
170.82.188.2	181.162.40.73	181.161.84.187	186.148.42.246	191.112.34.152	201.215.184.66
181.162.64.158	186.20.117.211	186.21.5.25	186.156.177.47	191.115.22.25	201.215.96.37
181.163.71.100	186.20.127.120	186.34.188.62	186.156.200.21	191.115.28.193	201.219.233.51
181.163.97.139	186.20.200.17	186.34.245.118	186.156.227.68	191.115.72.146	201.219.234.38
181.203.121.45	186.20.244.246	186.34.33.219	186.156.42.75	191.115.97.141	201.219.236.5
181.203.15.120	186.20.255.25	186.34.35.90	186.156.59.130	191.116.168.82	201.219.236.61
181.203.44.214	186.20.43.120	186.34.53.161	186.156.70.234	191.116.20.25	201.221.123.39
181.203.72.50	186.21.192.110	186.34.54.159	190.162.82.212	191.116.75.255	201.223.13.16
181.203.8.195	186.35.216.40	186.35.121.122	190.163.23.96	191.119.132.27	201.223.38.123
181.225.114.31	186.35.71.51	186.35.182.61	190.163.243.95	191.125.15.7	201.239.196.30
181.42.15.96	186.36.189.111	190.100.4.153	190.164.165.88	191.125.27.12	201.239.202.2
181.43.83.63	186.67.16.50	190.100.80.23	190.164.73.171	191.125.29.196	201.239.23.172
181.72.120.62	186.67.73.109	190.101.12.64	190.20.132.70	191.125.34.231	201.241.134.22
190.161.253.27	186.67.76.171	190.101.30.165	190.21.168.237	191.125.49.190	201.241.246.20

190.161.3.254	186.78.50.175	190.101.8.122	190.21.177.210	191.125.50.161	201.241.99.213
190.161.71.163	186.79.26.237	190.102.251.92	190.21.224.161	191.125.59.168	201.246.195.34
190.162.2.251	186.79.32.252	190.107.228.59	190.21.69.172	191.126.152.64	45.232.177.41
190.162.205.27	186.79.52.35	190.114.35.52	190.215.1.9	191.126.158.84	45.232.32.112
190.162.56.61	186.79.9.30	190.114.57.53	190.215.236.8	191.126.227.45	45.232.32.126
190.162.70.158	186.79.97.171	190.121.33.29	190.215.36.93	191.126.227.62	45.232.32.20
190.45.124.205	190.100.185.23	190.121.9.50	190.22.101.203	191.126.23.192	45.232.92.201
190.45.157.68	190.100.38.236	190.151.95.122	190.22.129.112	191.126.55.94	45.232.92.217
190.153.129.60	190.161.202.30	190.22.173.177	190.44.155.207	190.44.7.120	190.44.121.55
190.160.225.62	190.22.158.192	190.22.227.118	190.44.194.250	45.239.49.2	190.22.166.130
190.161.19.71					

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras), desde los sitios oficiales de los fabricantes.
- 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
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.09.05
15:14:27 -04'00'