ALERTA DE CIBERSEGURIDAD
"CSIRT Gubernamental"
Ministerio del Interior y Seguridad Pública

Equipo CIBERSEGURIDAD

Santiago, marzo de 2019

Santiago, 23 de marzo de 2019

COMUNICADO CIBERSEGURIDAD

(Actualización 1)

En base a informaciones recibidas de fuentes internas se ha establecido un estado situacional de alerta de ciberseguridad por incidente asociado a un malware denominado EMOTET que se encuentra afectado a sectores relevantes de la economía.

Se ha detectado complementariamente una vulnerabilidad de winrar. Dicho planteamiento se puede profundizar vía "CVE-2018-20250"[1]. Se recomienda bloquear este tipo de archivos temporalmente ".rar" y analizar el aplicativo en sus instalaciones.

Como producto de la coordinación intersectorial la información preliminar que se ha logrado recabar permite establecer que se debe bloquear, hasta que no se indique lo contrario mediante comunicado de igual o superior naturaleza, las siguientes URL y las siguientes direcciones IP:

Sitio web:

triosalud.cl

hxxp://5.39.218[.]210/dns/dns.php?dns=<random>"

hxxp://5.39.218[.]210/dns/logs/logpc.php

hxxp://185.29.8[.]45/1.exe

Archivo potencialmente malicioso:

http://www.triosalud.cl/wp/wp-content/uploads/2019/02/denuncias.rar

https://www.triosalud.cl/wp/wp-content/uploads/2019/03/tictic.txt

Direcciones IP anexas al final de este reporte. Anexo 1.

El bloqueo debe efectuarse tanto para flujos que provengan desde esos orígenes como flujos cuyo destino sean estos.

[1] https://nvd.nist.gov/vuln/detail/CVE-2018-20250

A nivel de RCE se están aplicando las protecciones respectivas y se ha elevado el nivel de alerta para estos patrones maliciosos.

Se notificará a los encargados de ciberseguridad en la medida que se detecte algún patrón que los involucre directamente para que se tomen las medidas del caso.

Otro comunicado, de no mediar una variación sustantiva de la situación, se emitirá para el restablecimiento del estado de normalidad en la RCE.

Referencias en medios a la fecha:

https://www.df.cl/noticias/mercados/banca-fintech/autoridades-y-bancos-en-estado-de-alerta-por-incidente-de-ciberseguridad/2019-03-22/230946.html

https://www.csirt.gob.cl/csirt-informa-sobre-alerta-de-ciberseguridad-de-malware-emotet/reportes/

https://www.latercera.com/pulso/noticia/bancos-reportan-sbif-presencia-malware-sistemas-computacionales-clientes-segmento-empresas/583244/

https://www.emol.com/noticias/Economia/2019/03/23/942165/Asociacion-de-Bancos-confirma-la-limitacion-temporal-del-acceso-a-los-canales-de-servicio-remotos-para-empresas-por-malware.html

Anexo 1: Lis de IP a bloquear por señales EMOTET

101.50.1.11

104.227.146.249

104.236.24.85

104.5.49.54

105.184.219.102

105.225.161.70

105.226.195.36

107.10.139.119

107.14.73.68

107.180.41.170

107.6.16.60

108.167.137.119

108.167.189.81

108.188.116.179

109.104.79.48

109.73.52.242

112.120.68.71

112.78.2.101

115.71.233.127

116.240.3.27

117.197.124.51

118.175.93.254

118.69.186.155

119.59.104.39

120.150.206.156

120.63.148.9

123.58.177.132

131.107.255.255

133.242.156.30

133.242.208.183

134.0.11.93

134.119.253.110

136.56.103.201

138.201.140.110

138.68.139.199

139.162.151.141

139.59.19.157

139.59.242.76

139.59.243.105

143.95.159.228

144.76.117.247

144.76.182.194

147.135.210.39

148.69.94.166

152.171.65.137

153.122.32.44

153.122.38.158

159.134.198.151

159.65.76.245

162.104.1.255

162.215.248.24

162.221.187.186

162.241.252.134

165.227.213.173

167.114.210.191

170.239.87.249

170.239.87.63

172.241.113.30

173.177.157.7

173.201.192.158

173.201.192.229

173.201.193.129

173.203.187.14

173.248.147.186

173.252.33.186

173.255.196.209

173.255.250.241

173.50.48.59

173.94.53.3

174.70.176.45

175.195.100.9

17.56.136.197

176.205.111.228

176.22.253.218

176.9.9.46

177.242.215.65

178.162.201.213

178.201.186.245

178.210.92.160

178.254.31.162

178.62.37.188

178.78.64.80

178.92.73.34

181.143.194.138

181.16.4.180

181.167.49.76

181.169.58.108

181.171.28.140

181.211.11.171

181.228.211.100

181.229.155.11

181.23.229.192

181.27.126.228

181.29.214.233

181.30.70.98

181.40.122.122

181.45.45.132

181.48.19.4

181.54.202.80

181.56.165.97

181.61.221.146

182.50.135.84

184.106.54.10

184.149.48.160

185.179.26.97

185.38.216.84

185.86.148.222

185.94.252.3

186.113.255.229

186.129.174.150

186.137.133.132

186.138.205.189

186.1.5.138

186.15.60.167

186.190.192.84

186.19.36.126
186.3.188.74

186.4.234.27

186.46.255.217

186.64.175.137

186.67.88.242

186.90.155.228

187.137.111.0

187.144.78.190

187.147.153.225

187.163.174.149

187.163.213.124

187.163.49.123

187.178.233.96

187.189.195.208

187.192.133.210

187.207.188.248

187.207.58.148

187.207.72.201

187.236.143.141

187.247.125.144

187.84.237.195

189.129.160.167

189.130.50.85

189.154.155.174

189.159.119.242

189.163.44.44

189.173.4.161

189.190.40.163

189.193.88.137

189.208.126.53

189.208.239.98

189.213.205.70

189.230.171.255

189.250.100.248

189.250.145.98
190.107.177.246

190.112.197.130

190.112.228.47

190.117.206.153

190.120.22.227
190.138.221.70

190.146.158.142

190.146.214.85

190.146.86.180

190.15.198.47

190.17.173.58

190.185.241.151

190.190.101.38

190.195.169.170

190.196.70.188

190.210.3.93

190.211.207.11

190.226.34.8

190.226.40.3

190.233.119.42

190.245.10.162

190.25.255.98

190.55.123.250

190.6.24.248

190.97.120.3

190.97.219.241

191.252.112.194

192.155.90.90

192.163.199.254

192.185.179.127
192.185.79.58

192.226.247.73

194.183.83.82

194.85.67.180

196.210.47.216

197.88.29.182

198.199.185.25

198.50.180.210

198.54.117.200

198.74.58.47

199.188.66.157

199.244.76.149

199.79.62.243

199.79.63.83

200.113.185.229

200.116.26.234

200.194.26.234

200.24.248.194

200.43.114.10

200.45.191.16

200.50.177.218

200.50.185.54

200.58.111.121

200.58.111.206

200.58.118.149

200.59.145.85

200.59.189.70

200.71.37.207

200.83.21.5

200.86.246.50

201.103.81.129

201.200.3.74

201.212.49.246

201.212.7.96

201.220.152.101

201.231.70.72

201.236.95.82

201.239.154.191

201.251.43.69

201.97.58.156

202.134.191.142

202.162.242.9

203.124.10.231

203.143.82.157

203.143.86.111

203.198.129.4

207.167.198.23

207.255.59.231

208.180.149.228

208.180.246.147

208.78.100.202

209.141.57.94

209.159.244.240

209.200.251.20

209.213.232.117

209.249.170.98

209.86.93.202

210.19.41.87

210.2.86.72

210.2.86.94

211.115.111.19

212.122.71.196

212.227.15.179

212.81.22.231

213.107.110.253

213.186.33.3

213.186.33.40

213.229.190.236

216.154.222.52

216.176.21.143

216.218.93.187

216.251.1.1

216.252.83.23

216.40.42.5

216.70.64.80

217.13.106.160

217.13.106.203

217.145.83.44

217.16.7.149

217.174.206.181

219.94.254.93
220.123.35.12
222.214.218.192

23.254.203.51

24.137.254.148

24.222.22.58

24.243.101.134

24.3.178.228

24.51.106.145

24.59.228.182

31.172.86.183

31.193.130.187

31.53.229.12
23.16.101.217

37.120.175.15

37.187.216.196

37.210.168.251

38.131.14.154

39.112.243.65

45.123.3.54

45.224.52.174

45.33.49.124

45.42.31.50

45.59.204.133

45.63.17.206

45.70.90.134

45.73.27.218

45.76.123.144

46.163.76.187

47.14.41.119

47.180.177.96

49.212.135.76

50.116.63.9

50.21.147.8

50.246.45.249

50.31.0.160

50.80.248.108

50.87.147.17
75.101.152.133

51.255.50.164

51.52.210.9
35.230.147.17
95.32.65.50

54.173.129.2

58.171.215.214

59.102.162.24
65.9.128.163

59.23.248.48

62.75.187.192

62.75.191.231

63.77.201.245

64.13.225.150

64.95.245.82

65.99.252.110

66.147.240.154

66.147.242.164

66.206.5.26

66.209.69.165

66.96.147.100

66.96.147.144

66.96.186.2

67.184.210.222

67.205.149.117

67.212.42.233

67.237.41.34

68.14.221.174

69.158.10.125

69.163.33.82

69.195.223.154

69.198.17.20

69.198.17.7

69.65.33.119

69.8.25.109

70.184.97.144

70.28.22.105

70.28.3.120

70.50.196.234

70.55.70.147

70.57.82.196

70.60.50.60

71.11.157.249

71.43.73.58

71.88.106.124

72.161.250.4

72.214.54.39

72.47.248.48

72.84.82.20

73.183.131.231

73.57.148.230

74.202.142.71

74.208.5.13

74.208.5.15

75.126.5.21

75.128.237.42

75.99.13.124

76.65.107.103

76.90.224.32

77.44.98.67

78.186.26.189

78.186.5.109

78.188.105.159

78.46.5.205

78.47.182.42

79.170.40.139

79.66.242.43

79.98.31.206

80.12.84.86

80.153.203.197

80.78.250.34

81.7.10.106

81.93.1.69

82.78.228.57

83.103.164.123

83.222.124.62

84.200.106.120

85.104.59.244

85.54.169.141

86.109.170.57

86.122.149.86

86.98.71.253

87.106.139.101

87.106.210.123

87.140.80.252

87.201.127.70

87.236.16.126

87.236.16.166

87.236.16.4

89.184.78.159

89.186.26.179

89.186.26.180

89.211.193.18

89.252.182.3

91.136.8.160

91.195.240.117

91.205.215.57

92.48.118.27

94.63.172.7

94.76.200.114

95.141.175.240

95.211.209.209

95.216.188.43

95.78.115.115

95.9.248.89

96.22.189.104

96.246.206.16

98.100.134.133

98.102.182.2

98.142.208.27

99.234.31.250

//

Control de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V1.0	22/03/2019	CSIRT	Creación	-
V2.0	23/03/2019	CSIRT	Agrega anexo, y ajustes menores de redacción.	Nuevos antecedentes del incidentes
V2.0	23/03/2019	CSIRT	Anexo 1	Se corrige errores en importación de IP's desde txt
		CSIRT		
		CSIRT		

Tabla 1 - Tabla gestión de cambios