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

Equipo CIBERSEGURIDAD

Santiago, marzo de 2019

Santiago, 22 de marzo de 2019

COMUNICADO CIBERSEGURIDAD

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 que uno de los potenciales vectores de distribución está asociado a una vulnerabilidad de winrar. Esa se puede profundizar vía “CVE-2018-20250”.

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

Achivo 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:

190.107.177.246

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

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.

Control de Cambios

Versión cambios	Fecha emisión	Autor cambios	Referencia, sección o capítulo modificado	Motivo de modificación
V1.0	22/03/2019	CSIRT		-
		CSIRT		
		CSIRT		
		CSIRT		
		CSIRT		

Tabla 1 - Tabla gestión de cambios