Alerta de seguridad informática	2CMV20-00051-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 de Marzo de 2020

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), ha identificado una campaña de malware a través de un correo electrónico que utiliza el nombre de la Tesorería General de la República.

El mensaje del correo indica que según la información entregada en los noticieros del canal público, a partir del 27 de marzo de 2020 comenzará la liberación del pago a los pensionados por concepto de contribuciones e informa que los contribuyentes que han realizado sus pagos a tiempo serán premiados con un descuento del 70% durante 3 meses. El atacante intenta persuadir a la potencial víctima que solo a través del enlace adjunto y que ingresando su rut podrá saber si es beneficiario de este descuento. Al ingresar al enlace se descarga un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión ejecutable MSI. Al ser ejecutado, se realiza un proceso falso de instalación, pero en realidad se gatilla un script que descarga el malware.

Indicadores de compromisos

Servidor Smtp

[185.98.147.73]
[5.83.0.14]
[5.83.0.13]
[185.98.147.54]
[185.98.145.188]
[185.98.147.32]
[167.89.100.141]
[167.89.100.140]
[50.31.60.24]
[167.89.100.132]
[50.31.60.236]

Sender

emblue3prd_ctc@emark4[.]embluejet[.]com

Asunto

TGR – Liberación de pago

Url's

http://u4208939[.]ct.sendgrid[.]net/ls/click
https://www[.]chaiyaphummunicipality[.]com/docs/stum[.]tdr

Archivos adjuntos

Archivo : TGR0903.zip
MD5 : 08ab7460137955cec0b63d33efb81859

Archivo : TGR0903.msi
MD5 : 3e8ee8a0ae092d4333296dd1f8b2b7ee

Archivo : stum.tdr
MD5 : f2b44aa09d25a254b3a918522c8490ee

Archivo : P6FIVPRV7G5A0K8LDL8PZ9HZNKCFQ1RD
MD5 : 2126b7d7e22820d87487d81aa3929ec9

Archivo : YRP6XF3X0SBKGQBE94GMEYSSN2
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Archivo : EARP7Z12LMV2GUAPK8H8Z4ZT9MJ34
MD5 : dbc12f8dcb8f62a67e016dc231497be8

Imagen Mensaje

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.10 18:52:25 -03'00'