Alerta de seguridad informática	2CMV20-00048-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de febrero de 2020
Última revisión	10 de febrero 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 que indica que posee mora en un pago (no indicando cual entidad).

En el mensaje del correo se visualiza una imagen de la supuesta cuenta impaga, al hacer click en el adjunto, se descarga un malware el cual se ejecuta en el equipo víctima infectándolo con Emotet.

Indicadores de compromisos

Servidor Smtp

[40.92.10.20]

[40.92.10.29]

[40.92.10.85]

[40.92.10.105]

Sender

lmejiara[@]hotmail[.]com

auramar441[@]hotmail[.]com

t.otoy00[@]hotmail[.]com

Nota5contabilidad[@]hotmail[.]com

Asunto

Aviso importante, realice sus pagos a tiempo.

Urls:

http[:]//217[.]8[.]117[.]64/tal[.]exe

http[:]//217[.]8[.]117[.]64/theCC/cred[.]dll

http[:]//217[.]8[.]117[.]64/theCC/index[.]php

IP

[217.8.117.64]

Archivos adjuntos.

Archivo : Fecha_de_pago_10_FEB_PDF.tar.z

SHA256 : 7118A3E214A6CA334482847983D277ED1758BE2698DC1C8818EE96E9F8FB4EA1

Archivo : Fecha_de_pago_10_FEB_PDF.tar

SHA256 : E665063E211A4CB1B9CAB567768963250211CB173764197545D678632D84E259

Archivo : Fecha de pago 10 FEB PDF 0168385053359289450475728503548674625122487405372619382464910778330865O.exe

SHA256 : F332039F100DA6D85CE5DA33BBC4B1128188E58B1BB28CBA226BBCB11642F1AC

Archivo : gvsaa.exe

SHA256 : F332039F100DA6D85CE5DA33BBC4B1128188E58B1BB28CBA226BBCB11642F1AC

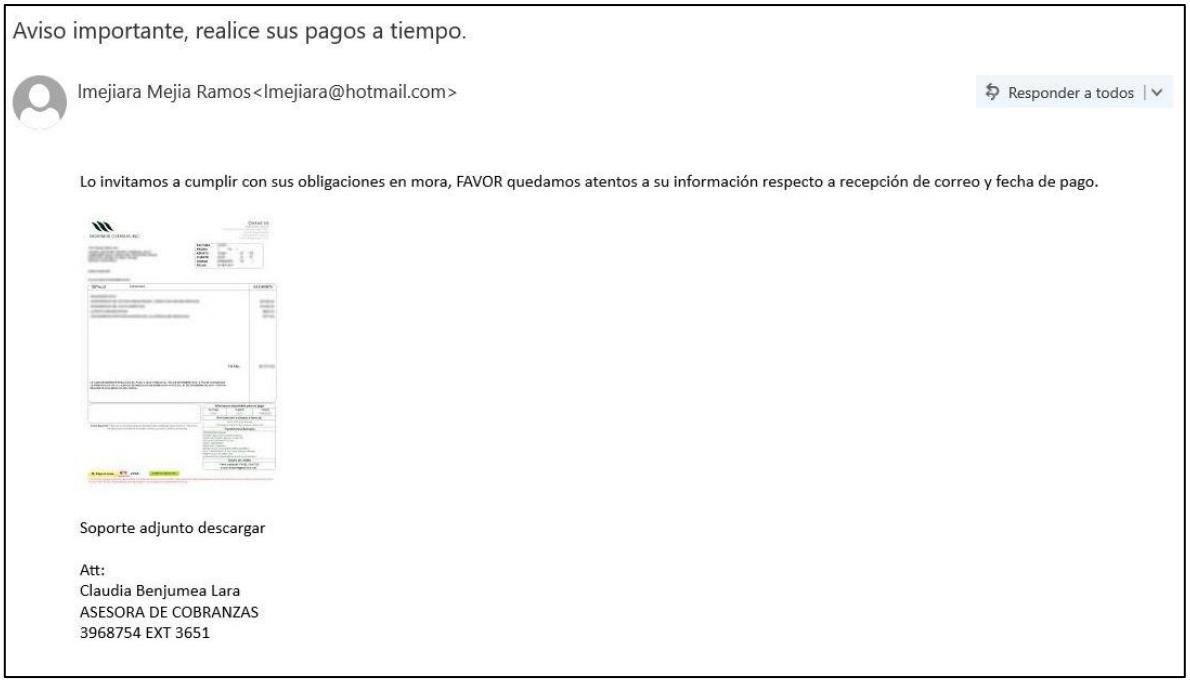
Archivo : cred[1].dll

SHA256 : 9D2B7780F2F0B9B321752D01E3E12B447E26BCD11E913FF6251E81677AB4A27B

Archivo : tal[1].exe

SHA256 : 963ABE7AA94C8B3E12E231E10C62BA00E3F89948EDB77E017CB2EB25BC24CA56

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: 2020.02.10 15:22:07 -03'00'