Alerta de seguridad informática	2CMV20-00043-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2019
Última revisión	25 de Enero 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), ha identificado una campaña de malware que utiliza el nombre de la Compañía de Telecomunicaciones Entel.

El mensaje del correo indica que ha ocurrido un imprevisto en el pago de la cuenta del cliente, argumentando un problema asociado Rut denominado “valores en abierto”. Al confuso mensaje se agrega un enlace a una factura, para la cual se solicita utilizar Windows. Al momento de seleccionar el enlace se descarga un archivo Zip. Al descomprimir 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
[195.123.222.253]
[195.123.222.252]
[217.12.201.201]

Sender
root@bt.com

Asunto
Creemos que ha ocurrido algún imprevisto con el pago de su cuenta

Url's:
http[:]//bloggingandme[.]com/wp-admin/th09xv-952-777431893-aeyna5j-mej4ry1dc/
http[:]//vergaralandscaping[.]com/home/docs/download/opsessentaeoi8[.]ghr

Archivos adjuntos.
Archivo : Vierw-RR.zip
MD5 : 1dc1a2699a6297788a99b294892e624f

Archivo : Vierw-RR.msi
MD5 : 331311740ae5b440f7edfc5a267a72c0

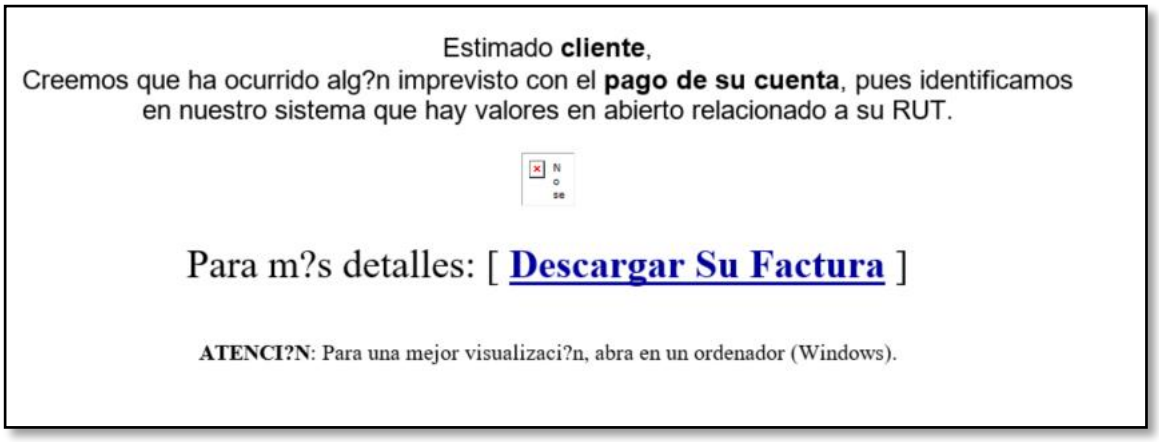
Archivo : opsessentaeoi8.ghr
MD5 : daefd9de21606ffd6553b26064a9b64b

Archivo : CJM2G0DG0Y3GJ39MEL8QQA1XP40BP251RZFRCMP
MD5 : a57205d24494d387d1175f8848ad86f9

Archivo : X2UDLWY6CN7XY3HVLVOTA9VZ57
MD5 : 2c48da37295c62e856d900f22002b058

Archivo : ZL00KRU9YV95U9YRVGYQV297X0YP0ESXIVXOAMCI
MD5 : c56b5f0201a3b3de53e561fe76912bfd

Imagen Mensaje


Estimado **cliente**,
Creemos que ha ocurrido alg?n imprevisto con el **pago de su cuenta**, pues identificamos en nuestro sistema que hay valores en abierto relacionado a su RUT.

Para m?s detalles: [**Descargar Su Factura**]

ATENCI?N: Para una mejor visualizaci?n, abra en un ordenador (Windows).

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: 2020.01.25 11:57:06 -03'00'