Alerta de seguridad informática	2CMV20-00052-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Marzo de 2020
Última revisión	13 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 Servipag.

El mensaje del correo indica que según la información entregada por teléfono, se envía el comprobante por este medio. El atacante persuade para que seleccione el enlace, para así ser dirigido a la descarga de un archivo ZIP. Una vez que se descomprime el archivo, se obtiene otro archivo con extensión .JS. Al ser ejecutado, se gatilla la descarga el malware.

Indicadores de compromisos

Servidor Smtp

[168.245.115.183]
[168.245.120.135]
[167.89.16.17]
[167.89.10.181]
[168.245.59.205]
[167.89.92.29]

Sender

@sendgrid.net

Asunto

De acuerdo con el contacto telefónico le estoy enviando el comprobante

Url's

http[:]//u15365113[.]ct[.]sendgrid[.]net/ls/click
http[:]//noticiasdelestado[.]xyz/
http[:]//webhost[.]dusit[.]ac[.]th
http[:]//sahakorn[.]dusit[.ac[.]th
http: //3[.]136[.]20[.]196/uff/MZX4GA C4C4ZCI65[.]php
[202[.]29[.}83[.]151]

Hash MD5

C56B5F0201A3B3DE53E561FE76912BFD
B3146B270253DED0D19514E3DF42AEDD

Archivos adjuntos.

Archivo : pqbGl2I5Llln5G.zip
MD5 : 98d335d58c28af67604fbc9a92bcb1b6

Archivo : pqbGl2I5Llln5G.js
MD5 : ce9d4a64555cda4b6c40318c1b2aa222

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: 2020.03.13 16:34:44 -03'00'