Alerta de seguridad informática	2CMV20-00056-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 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 indicando el pago de algún tipo de servicio. El mensaje del correo indica que se realizó una transferencia electrónica de fondos en la cuenta de quien recibe el correo. El atacante dispone un enlace en el cuerpo del correo, el que supuestamente permite descargar el comprobante del pago. Si una persona selecciona el enlace es dirigido a un sitio donde se descarga un archivo ZIP, la cual contiene un archivo MSI el cual, al ser ejecutado, gatilla un script que inicia la descarga el malware.

INDICADORES DE COMPROMISO

Servidor Smtp
[52.173.35.129]
[40.71.186.239]
[40.117.134.18]
[52.173.34.112]
[52.165.183.166]
[52.186.84.69]
[104.43.218.174]
[52.224.167.111]
[52.224.167.105]
[52.224.167.73]
[40.117.134.18]

Sender
root@boby33[.]borawebservicioscl[.]com
root@boby38[.]borawebservicioscl[.]com
root@boby36[.]borawebservicioscl[.]com
root@boby40[.]borawebservicioscl[.]com
root@boby16[.]borawebservicioscl[.]com
root@boby20[.]borawebservicioscl[.]com
root@boby25[.]borawebservicioscl[.]com
root@boby23[.]borawebservicioscl[.]com
root@boby06[.]borawebservicioscl[.]com

Asunto
envio de comprobante – TEF

Url's
http[:]//www[.]liliioui[.]com[.]br/heart/9418948910/230320/comprobante[.]php
http[:]//hearingable[.]com//wp-content/00078144/998894414541/index[.]php
http[:]//sahakorn[.]dusit[.]ac[.]th
172.217.9[.]206
202.29.83[.]151

Hash MD5
f652d8e718ffe071c3d39a13cff1803c
4bdb0590d6d666171801a87844b068af

IMAGEN DEL 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: 2020.03.25 12:58:56 -03'00'