Alerta de seguridad informática	**2CMV-00024-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**08 de Agosto de 2019**
Última revisión	**08 de Agosto 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 Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene de la Tesorería general de la Republica. Los delincuentes buscan engañar a los usuarios advirtiéndoles que existe una obligación tributaria que se encuentra impaga. Para visualizar el informe generado por el Servicio Impuesto Interno, un usuario debe descargar el enlace adjunto en el correo electrónico. Al ser ejecutado desencadena la infección del malware.

Indicadores de compromisos

Url's:

https://files[.]fm/pa/Jhon-Files/2019-08-07_aftbunyn/tesoreria_download[.]zip
https://files.fm/down[.]php?truemimetype=1&i=eqbgw6g4
http://docsecuredownload[.]com/status/?ACAO=descargar[.]cgi
http://tudonetclientes[.]website/controle2.php

Smtp Host

- [45.132.104.43]
- [91.211.250.234]
- [45.88.78.151]
- [45.88.78.147]

From: (Original)

- root@ubuntu.coma
- root@usd.com
- root@f.net
- root@c.com
- root@cook.com

Subject:

Aviso (TGR)

Archivos adjuntos

Archivo : tesoreria_download.zip
MD5 :
SHA256: c41553856a0f33a21c2841ad4487016e528d0e6e5c44377ae495a67dbf45c9ad

Archivo : tesoreria_download.msi
MD5 : 9f533b56bc4ad87ffa2295121b10df80
SHA-256 : c737fee428ac17a8996c2c6aeade42ee8e5bebd1702e0667c5d102654be2c10a

Archivo : shfolder.dll
MD5 : 128564879f5aa7174ef77e2472f120c9
SHA-256 : 5c3b86a868b3358e617905a34aa84034c8e06bf50275810f5c0e9425d64a8c50

Imagen Phising de Correo

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: 2019.08.08 08:21:23 -04'00'