Alerta de seguridad informática	**2CMV-00035-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**23 de Octubre de 2019**
Última revisión	**23 de Octubre 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 criminales buscan engañar a los usuarios advirtiéndoles sobre una supuesta liquidación tributaria impaga. A la potencial víctima se le ofrece la posibilidad de descargar desde un enlace el informe generado por el Servicio de Impuesto Internos. Al seleccionar el hipervínculo se inicia el proceso para la descarga del archivo malicioso. Junto a este informe se adjuntan indicadores de compromiso.

Indicadores de compromiso

Url's:

http[:]//copiasul[.]com[.]br/error
http[:]//copiasul[.]com[.]br/erros/index2[.]php
http[:]//copiasul[.]com[.]br/wrapper-bin/index2[.]php
http[:]//18[.]209[.]163[.]113/cont/puma[.]php
http[:]54[.]198[.]30[[.]]41/v
http[:]//copiasul[.]com[[.]]br/wrapper-bin/shoy/amyst3rd[.]jab

Sender

mmca@64149hpv095002[.]ikoula[.]com
server2@srv-8063[.]devcloud[.]hosting[.]acquia[.]com
server3@srv-8064[.]devcloud[.]hosting[.]acquia[.]com
server7@srv-8068[.]devcloud[.]hosting[.]acquia[.]com
server6@srv-8067[.]devcloud[.]hosting[.]acquia[.]com
server4@srv-8065[.]devcloud[.]hosting[.]acquia[.]com
server5@srv-8066[.]devcloud[.]hosting[.]acquia[.]com
bitarafhaber@bitarafhaber[.]com[.]tr
hastenllc@srv194[.]prodns[.]com[.]br

Smtp Host

i1775-198.members.linode[.]com	[172.104.184.198]
li473-9.members.linode[.]com	[176.58.108.9]
host-185-59-31-167.ttnetdc[.]com	[185.59.31.167]
li1823-170.members.linode[.]com	[172.104.246.170]
epsilon.imcconseil[.]fr	[178.170.95.2]
gateway33.websitewelcome[.]com	[192.185.146.195]
gateway33.websitewelcome[.]com	[192.185.145.24]
host-185-59-31-167.ttnetdc[.]com	[185.59.31.167]
acquiamail10.acquia[.]com	[173.203.82.6]

Subject:

Tesoreria General de la Republica

Archivos

Nombre : TGR-1321357581_.zip
MD5 : 55b6a3e71153efa0e02094383e604fd9

Nombre : TW9069119609.msi
MD5 : 8cd4b8acc4b112d02237010616f4843c

Nombre : aMyst3rD.jab
MD5 : c4168ef94fbfbfe4a1f8d63a27312b92

Nombre : I8TMIRB7F1XNQEIB4M8GGTC0OK8SHZUPQSG3T3
MD5 : b6de746a05f56afa69f9615b047705c5

Nombre : Q6M8XFKV4INKV5KHHEYL4510KU31F
MD5 : 1d864318c347f24c4b0d30380bd9efb6

Nombre : YDOKWVU4UP303WP7AQK04Q7X1768JWPE
MD5 : c56b5f0201a3b3de53e561fe76912bfd

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: 2019.10.23 19:30:03 -03'00'