Alerta de seguridad informática	**2CMV-00036-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**25 de Octubre de 2019**
Última revisión	**25 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 Empresa de Courier Nacional e Internacional Chilexpress. Los cibercriminales buscan engañar a los usuarios informándoles sobre la existencia de un paquete en sus depósitos, adjuntando un código de seguimiento. Lo anterior busca incitar a las víctimas para realizar un seguimiento del supuesto pedido a través del enlace. Al seleccionar el hipervínculo, la víctima es redireccionada automáticamente hasta descargar el archivo malicioso e infectarse con un malware bancario. Se adjuntan los indicadores de compromisos.

Indicadores de compromisos

Url's:

http[:]54.198.30[.]41/v
http[:]54.198.30[.]41/tgr
http[:]//env-8651008[.]users[.]scale[.]virtualcloud[.]com[.]br/0ldtats[.]jek

Smtp Host

li1961-110.members[.]linode[.]com	[172.105.7.110]
li1971-177.members[.]linode[.]com	[172.105.16.177]
li1702-14.members[.]linode[.]com	[172.104.92.14]
li1584-35.members[.]linode[.]com	[139.162.100.35]
li1699-174.members[.]linode[.]com	[172.104.89.174]
li1584-35.members[.]linode[.]com	[139.162.100.35]
li1872-153.members[.]linode[.]com	[172.105.218.153]
li1775-198.members[.]linode[.]com	[172.104.184.198]
li473-9.members[.]linode[.]com	[176.58.108.9]
li593-196.members[.]linode[.]com	[151.236.222.196]

Subject:

Tenemos un pedido en nuestro depósito en su nombre

Archivos

Nombre	:	QCWNAV800375.msi
MD5	:	34df028364cd19d4e84abe343803f74d
Nombre	:	0ldtats.jek
MD5	:	81b8a1fb2cacc223c6a481c05761b4bc
Nombre	:	BNB3A6Z7APWN48Y8BIV1KLP0U4H5ZF7I2AVUE
MD5	:	1cef96e373cd8641b51a5a48b35fd9d5
Nombre	:	DG7AVLQ4J2OB7AJO3T48PZF5UVE
MD5	:	412c34d15922246ab5c8cf04327e2760
Nombre	:	NRYX8S2Y6INF3MRG1PQMFG24PUFNA7
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: 2019.10.25 11:34:17 -03'00'