Alerta de seguridad informática	**2CMV-00033-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing - Malware**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**01 de Octubre de 2019**
Última revisión	**01 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 delincuentes 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, la víctima es direccionada automáticamente hasta el archivo malicioso. Este archivo, al ser ejecutado genera un proceso de instalación. Luego de la instalación, se genera una conexión a internet descargando un supuesto documentos Word, pero en realidad es un archivo Zip que contiene tres archivos más. Se adjuntan los indicadores de compromisos.

Indicadores de compromisos

Url's:

http[:]//www[.]tokenschile[.]com/public/?acao=descargar[.]cgi
https[:]//files[.]fm/pa/account-business/2019-09-30_c4veawtd/business_tesoreria[.]zip
https[:]//files[.]fm/down[.]php?truemimetype=1&i=serb96qc
http[:]//filesdocuments[.]com/documentOP3[.]doc
http[:]//51[.]15[.]249[.]181

Smtp Host

[185.206.214.129]
[185.206.214.121]

Sender

root@r[.]com

Subject:

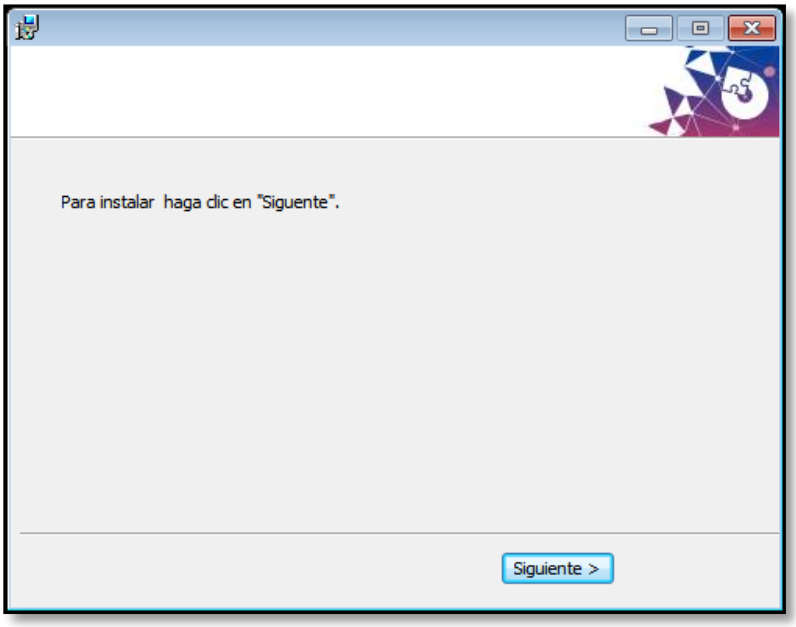
Aviso (TGR)

Archivos adjuntos.

Nombre	:	business_tesoreria.msi
MD5	:	84a2c2d4a435bff6809399229236e7e0
Nombre	:	documentOP3.doc (zip)
MD5	:	d13ba3428e19489d635066c3024ab429
Nombre	:	F0Z3TNE1EOAZB24ZZWSFD6CON13X9O.dll
MD5	:	0cbdca5d50c9bd6ffb1387921f37bc18
Nombre	:	T6ERC5ECZL5V0MEHI1B1AEE7SZCS4.EXE
MD5	:	c56b5f0201a3b3de53e561fe76912bfd
Nombre	:	BFVUCX3T5T4UPAUZW3LWEFWBUNMP5
MD5	:	60077c43751f4e160f38ccb0df5f3d54

Imagen Phising de Correo

Imagen de Instalación



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: 2019.10.01 09:49:40 -03'00'