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), con la colaboración Centro Nacional de Ciberseguridad de la Policía de Investigaciones de Chile, ha identificado nuevos indicadores de compromisos de la campaña de phishing con malware asociado informada recientemente en la alerta 2CMV-00033-01.

La campaña es perpetrada a través de un correo electrónico que supuestamente proviene de INTERPOL, correo que supuestamente es enviado desde una casilla de correo electrónico de la Policía de Investigaciones de Chile.

Los criminales buscan engañar a los usuarios advirtiéndoles que existe un proceso criminal a su nombre, ofreciendo la posibilidad de descargar la información sobre el caso en el enlace que acompaña el texto del correo. El archivo, al ser ejecutado, se instala y genera una conexión a internet descargando un supuesto documento Word, pero en realidad es un archivo Zip que contiene tres archivos más. Se adjuntan los indicadores de compromisos.

Nuevos Indicadores de Compromisos

Url's:

http://www[.]filesdocuments[.]com/docop4[.]doc

Archivos Adjuntos.

Nombre	:	segundo_aviso.zip
Sha256	:	12f6ed0ff0db62ddb3e31fcf1c1b8509
Nombre	:	segundo_aviso.msi
MD5	:	12f6ed0ff0db62ddb3e31fcf1c1b8509
Nombre	:	docop4.doc (zip)
MD5	:	4d498ae8e98888c43803af5f6072a5f9
Nombre	:	QKNM5NMWZO2OKDWPK3COLF1PKYJ8CI4BZ28.dll
MD5	:	082163b6bc7a8896d535731874c8d191
Nombre	:	VJ6HHB14GA6MKWJNZ0615VH3M2
Sha256	:	236fad4d70cb38a38fd64498cad8fc40
Nombre	:	Y79IVWDNW95AXJYRNC41RN49QWGCIS1VJLK23.exe
MD5	:	c56b5f0201a3b3de53e561fe76912bfd

Smtp Host

[77.220.213.246]
[77.220.213.78]
[212.86.109.144]
[185.203.240.71]

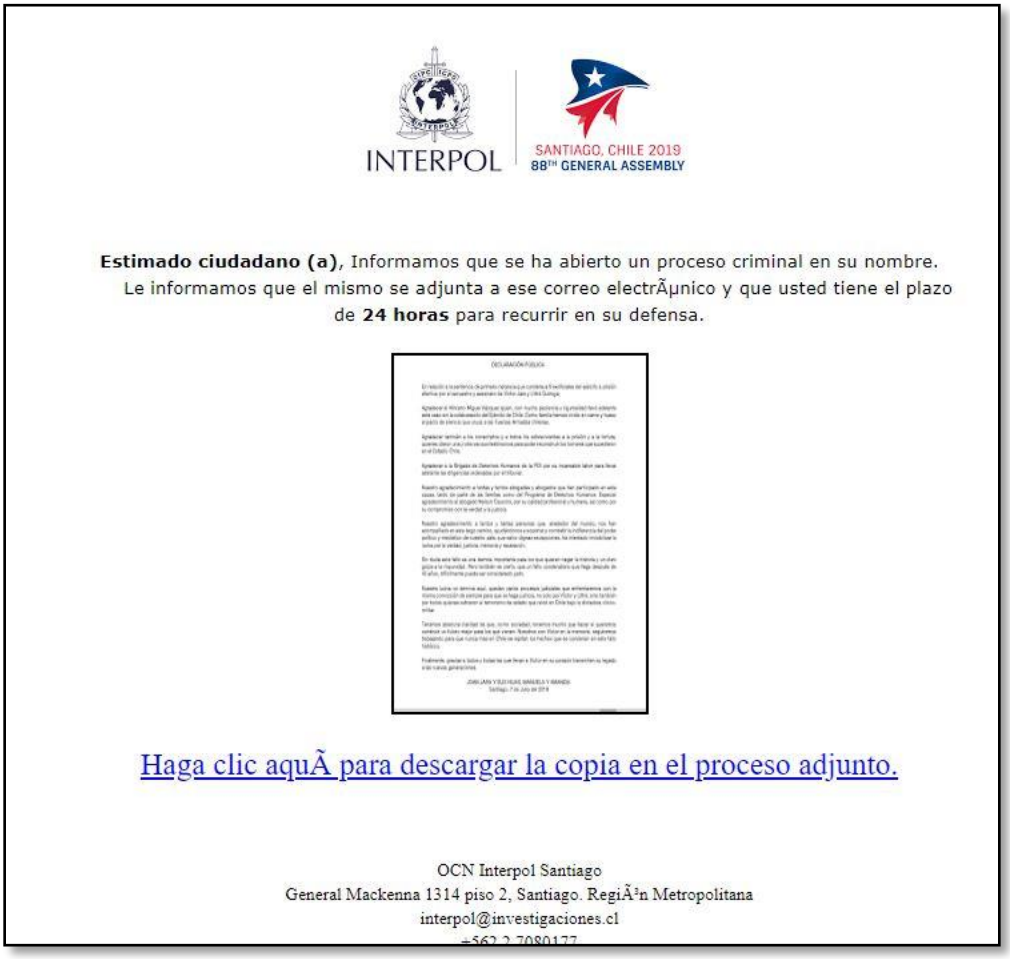
Sender

root@order[.]com

Subject:

Segundo Aviso

Imagen Phishing de Correo



Reporte Anterior

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:

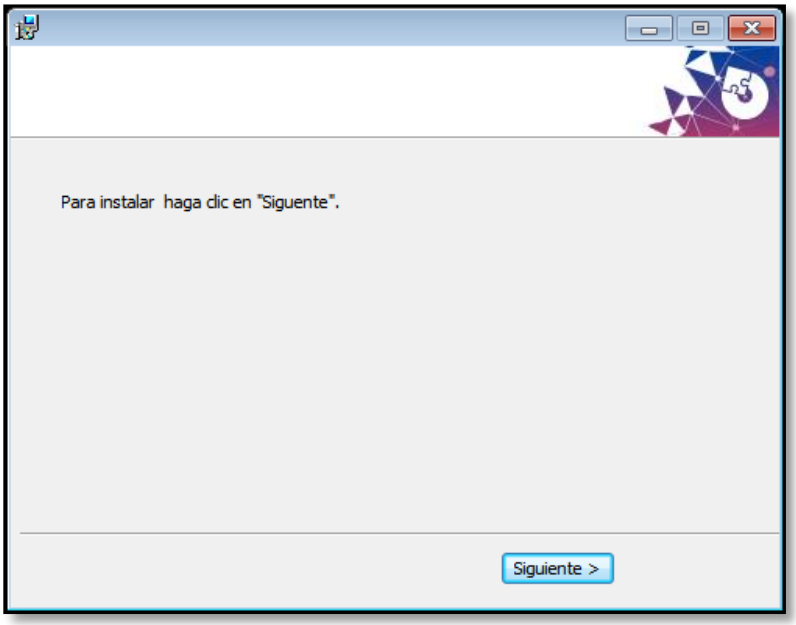
Aviso (TGR)

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 Phishing 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 18:21:15 -03'00'