Alerta de seguridad informática	2CMV21-00174-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2021
Última revisión	10 de mayo de 2021

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 de Gobierno), ha identificado una campaña de malware supuestamente proveniente de Tesorería General de la Republica. El atacante busca persuadir a las personas para descargar el archivo adjunto y ser ejecutado.

El mensaje del correo indica Informa que existen obligaciones tributarias que se encuentran impagas. El atacante adjunta un vínculo redirige al usuario a varios enlaces, para luego descargar el malware y ejecutarlo en su equipo, donde gatillará la infección del dispositivo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidores SMTP
li895-197.members.linode.com [45.56.93.197]
li225-12.members.linode.com [173.255.215.12]
li1857-222.members.linode.com [172.105.203.222]
[icecube.xtardns.com] [144.76.5.176]
[li1885-121.members.linode.com] [172.105.231.12]
[icecube.xtardns.com [144.76.5.176]

Correo Electrónico

director@cigiden.cl	(Suplantada)
csanmart@ing.udec.cl	(Suplantada)
covalle@inia.cl	(Suplantada)
liliana.pulgar@gmail.com	(Suplantada)
Informacion_tgr10901914@tgr.cl	(Suplantada)
maidas@cnet.com	(Suplantada)
Oficina_Sii13114046@sii.cl	(Suplantada)
TGR-43947041@oficina.cl	(Suplantada)

Asunto
Tesoreria General de la Republica TGR
Regularizacion de un pago no ingresado N
Regularizacion de un pago

IoC URL

http://www.neuewegezumwasser[.]de/images/logo/mail/?/id/AQQkADAwATYwMAItMTMyNi0zNDdlLTAwAi0wMAoAEAC2%2BFDswJxTSrI80gwgzDtE

http://www.tenisecia.com[.]br/css/download/dow.php?

https://novohostpqp.s3-eu-west-1.amazonaws[.]com/htphuijex4cuar8i5n6vhml9gybgdnaz.zip

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre : aVpUqbjZsuOWmK2H97AiPrdxogtYeS.zip
SHA256 : 9320A80F15B11F981DA5CB831D06408EC6FEE620407202F446BC7A3DAC13794C

Nombre : TGR_FF0021S707T200800GHX.msi
SHA256 : 9C5E4442E24D03738140EC434D4A5B99367BE5542D71FBD9B5AFEB80008D8643

Nombre : htphuijex4cuar8i5n6vhml9gybgdnaz.zip
SHA256 : AB473D07504FBD2E9F071F9ABCD419BAF4671C17D893BCB84F41348CB23D5195

Nombre : lx3SEB230VC7b941DMxPY36S
SHA256 : C16C6DEF9C3753EA441E317E16649C0CB6CE9E5544E92B55A97715182D4FC78E

Nombre : MAjGV2xm2topgzUgBhuOc3bDk
SHA256 : 20691095F8E73E8F1910CD88542FF81ADB40B23AF4AF133D7B9CFB2FAA08692E

Nombre : PGHPGHZGEn.dll
SHA256 : B28479201FC52376BB5C979E562B77695D6DE5A41A14E847B8AF8900BC69ECD2

Imagen del mensaje

Estimado(a) Contribuyente

Tesoreria General de la República (TGR) : Le informa que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga. Una liquidación tributaria corresponde a la determinación de diferencias de impuesto detectadas por el SII. Puede descargar el informe generado por el SII en el siguiente enlance:

Informe de cobranza N-0011244588

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.10 17:46:18 -04'00'