Alerta de seguridad informática	2CMV22-00295-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2022
Última revisión	27 de abril de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 phishing con malware. El mensaje que proviene, supuestamente, de la Tesorería General de la República (TGR) informa que existen obligaciones impagas y que puede revisar el informe generado por la TGR en el archivo adjunto, ingresando la contraseña que se indica en el correo. Al descargar el archivo y ser ejecutado, se gatilla la infección del equipo

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto

✓ Tesoreria General de la Republica (TGR) informa que existen obligaciones pendiente.

Correo Electrónico

[lynxaviacao@lynxaviacao.com.br]
[sub1552_63@lin05.mandichost.com.br]
[meyers_bjoern@web.de]
[webmaster@24service.co.il]
[mw2pqgpp93@kawahara-law.jp]
[tipsadvi@host.inrunner.com]
[mssce@server.ony.oyo.mybluehostin.me]
[topmodatrend.com@topmodatrend.com]
[aannemingsbedrijfquakkelaar@aannemingsbedrijfquakkelaar.nl]

Servidor de correo

[lin05.mandichost.com.br]
[plesklinux01.mandic.com.br]
[cloud.stumpertjes.nl]
[vmi786999.contaboserver.net]
[sh11689.ispgateway.de]
[vmi827000.contaboserver.net]
[kawahara-law.jp]
[host.inrunner.com]
[server.ony.oyo.mybluehostin.me]
[mail188.sea71.mcsv.net]
[mail34.atl18.mcdlv.net]
[smtp17.itdchile.org]
[smtp20.itdchile.org]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: Tgr0014220.zip
SHA256: e13cce0cd9bd4f0854cc5413c7a55929155bfe2afe46247ee6763eb77635c645

Nombre: Tgr0014220.msi
SHA256: 2185765b437b0ac6b233605d00f8c98cb34c2e3154152522c02ee5c64d143ffc

Nombre: lock.txt
SHA256: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

Nombre: libeay32.dll
SHA256: cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: juik1.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: ssleay32.dll
SHA256: 754aadc3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f

Nombre: juik1.ahk
SHA256: 893ce8ba10a2c734921c1fe49219972fbb032dbcf7fb49d443031c639a4b21c4

Nombre: 6xhj17x312dlk2hwe718.zip
SHA256: cb6a6c3920daf4a5f84b89d80e9100f2dfbcec146ae3f4eefea526cf912aa086

Nombre: pZsRIYtYMH.aoc
SHA256: 728ec4e457500b7516fe73bbde00fbc4651db61961d666a235ef49b74154769f

Nombre: BbD8zqV52P6NX6Urjhhh
SHA256: c76a16d7e5909031501bdb1f4860d9ba4be17cd054ca04547dd5d6fc5299410d

Nombre: CBbglwxYQ2ej0fQ6veggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

IoC URL

hXXps://placade[.]jp/agt/--/https:/www.tgr.cl/?cliente=

hXXps://www.stt.eesc.usp[.]br/wp-content/languages/Tgr0014220.zip

hXXps://manuelruso[.]com/images/import/6xhj17x312dlk2hwe718.zip

Imagen del mensaje

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: 2022.04.27 17:08:12 -04'00'