Alerta de seguridad informática	2CMV22-00301-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de junio de 2022
Última revisión	09 de junio de 2022

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 phishing con malware. El mensaje que proviene, supuestamente, de la Tesorería General de la República (TGR) informa falsamente que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga, la cual corresponde a la determinación de diferencias de impuesto detectadas por el SII. Para revisar el falso documento, el atacante dispone un enlace para su descarga. Una vez que se descarga el archivo y es 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

✓Infoemail TGR - Atención Ciudadano, le Informamos sobre Deudas Pendientes a su nombre Verifique ahora. - (516512038694)

Servidor de correo

177.70.106.248
177.70.106.69
107.190.131.50

Correo Electrónico

lynxaviacao@lynxaviacao.com.br
sub1552_63@lin05.mandichost.com.br
rationalpolicies@linux.fitser.com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: TGR00214500011.zip
SHA256: 6a88340516602be1aa9e153ad2394cf1935213fd719cc0e4a378a75f17f051f3

Nombre: TGR00214500011.msi
SHA256: dc58e5c807762d9442e4d4b71921c56289081ddc2a367eabad30cca817686fa7

Nombre: lock.txt
SHA256: cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: lopp0.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: V7DX72X8SZDUJ1QW33.shi
SHA256: e9214d7c92555195443f2ac907302118992f3ea615ee0e0241152327534466c3

Nombre: c3rqf758ea72bx29tbmxhhh
SHA256: b988eebe4b1247db6c54519f59ff4e472f0de4b9e85bc6d62c54bfd7a6de3942

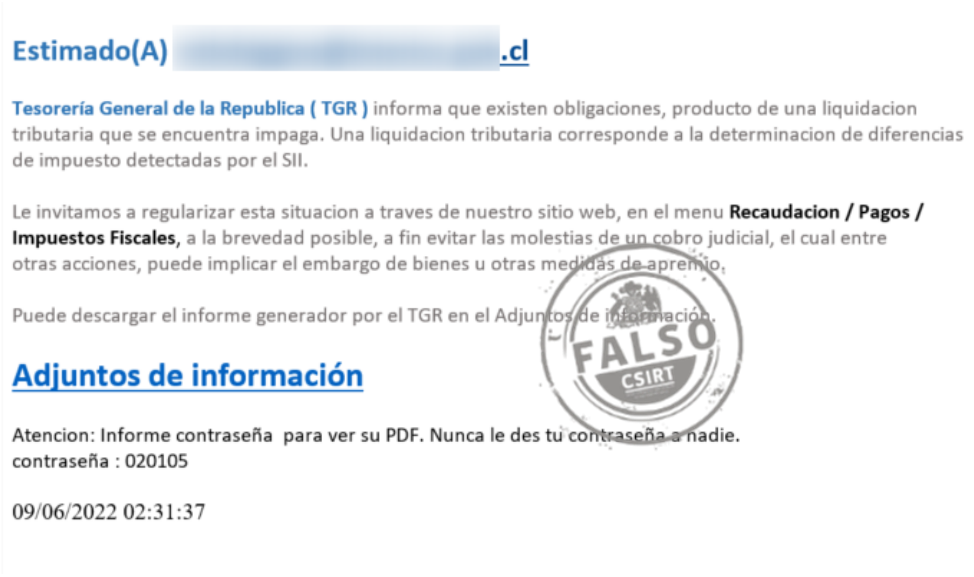
Nombre: mwgprakpoq.elh
SHA256: 28f24a369fd4c060cb4a77919861c62176a76f87e798b21cde9dc1c93b2af166

Dominios/URL:

kiamarketingbuzz.co[.]za
inservicemedia[.]com
anestis[.]info

https://kiamarketingbuzz.co[.]za/wp-content/languages/--/https:/www.tgr.cl/?cliente=intlohiggins@interior.gob.cl
https://inservicemedia[.]com/wp-content/uploads/--/TGR00214500011.zip
https://anestis[.]info/OLD/images/cloud/V7DX72X8SZDUJ1QW33.shi

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: 2022.06.09 14:53:28 -04'00'