Alerta de seguridad informática	2CMV21-00286-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de marzo de 2022
Última revisión	21 de marzo 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
Fw:enc: Informacion de Liquidacion Tributaria

Correo electrónico
mobilefirm@linux.itmonteur[.]net

Servidor de correo
[203.115.100.91]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: 003F101L4226B8017T0552S.zip
SHA256: 3316B967FFBE7806CCEC9E58C7991092BFD7BA35C8433B8D66BD2818AF6FB66B

Nombre: 003F101L4226B8017T0552S.msi
SHA256: 10D9650FF8F30F631DC5708F91171569A5EC1BFD00EBEF8856BC6C3F25CAEBCB

Nombre: software.exe
SHA256: 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

Nombre: software.ahk
SHA256: F0E24F78907C85916056A6E40C9B69D28B92C30038526FEE9CE2BE7C0C7686E7

Nombre: 8u21R0s5i361w01.zip
SHA256: 0B02777C821B11F24B3F01C2DA7D85319CCB624E907075798A8D0DBFC3CE5ABC

Nombre: R6B0lI94Fa7mNy7YyN6vvZJ7bbb
SHA256: C84B874E12794302DFE5507BC5E0BF21F64BC92357AD9382136A3EF66BB36244

Nombre: k2l0tQ99xY0bnzqCwwcaaa
SHA256: 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

IoC URL

http://3.144.108[.]13/imbox/
https://agtta.co[.]in/userfile/down/
https://dkloja.com[.]br/signup/file/8u21R0s5i361w01.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: 2022.03.21 17:32:09 -03'00'