Alerta de seguridad informática	2CMV22-00289-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de marzo de 2022
Última revisión	25 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
viv@viv.az

Servidor de correo
[159.69.42.89]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: 003128BF5055S9211EJ1K.zip
SHA256: 413ED7CDE5614D06671B4BDFD1176FE23BAB8FAD2D80367BF64A9342417FB034

Nombre: 003128BF5055S9211EJ1K.msi
SHA256 : 859128E61625516A7357BA6A3FACE1ED8F97C580DBC889CC0FCE520DC0072346

Nombre: djcn8.exe
SHA256 : 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

Nombre: djcn8.ahk
SHA256 : 55364E85CFBF30AFA459C5D7F62DF883E94E553CAE91CB7ED2309D1F6CB455BD

Nombre: JSON.ahk
SHA256: BB85E4530CCD6355B3EF3506548B4F513BEA844D1AF37A69624C9C455521C70F

Nombre: libeay32.dll
SHA256: CB7F180D74DD744FE32260026CC12D051AF0C5F6E1EF31ADC387773A1B44F967

Nombre: ssleay32.dll
SHA256: 754AADC3AA19E07F2BA20217DDB0412D90E686E9965100EC7DC16475DEA2077F

Nombre: b6c6zi5stehj19.zip
SHA256: ABDCDAE0F174DBBA566DB5DDA98371F380C885EFB589121DB8DED98209ADD2F2

Nombre: EDBEMnsnno.dll
SHA256 : 550B01B943A7C6696933CA06E3BC3A203F7FF9104BBBFA7A874E38BB65E5BC6F

Nombre: Vnkgv0588UlphQA71Dnrbbb
SHA256: D666B32D2C26CDDF295433F94A637E74DB0EEDB139F4941737F2E5DAFB1D1332

Nombre: w40J5mLLwvyi9hzWFW0Vaaa
SHA256: 3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4

IoC URL

http://13.38.30[.]133/imbox/?/mail/u/0/#inbox/FMfcgzGmvfRcvdVbKJNggqVtCPQwxqCT

https://w3tutors[.]com//sii/downlaod/#inbox/FMfcgzGmvfRcvdVbKJNggqVtCPQwxqCT

https://dkloja.com[.]br/signup/file/b6c6zi5stehj19.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: 2022.03.25 15:09:05 -03'00'