

Alerta de seguridad informática	2CMV22-0280-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2022
Última revisión	9 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 equipo CSIRT. La información contenida en los informes o comunicados está afectada 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 que proviene supuestamente del Servicio de Impuestos Internos, indicando falsamente que existen obligaciones impagas, por lo que se debe regularizar la situación.

Para convencer a la víctima, el atacante busca persuadir a las personas de descargar un falso informe originado por el SII con una contraseña que permitiría abrir el documento adjunto. De descargar el archivo y ejecutarlo, comienza 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: Informe de liquidación tributaria.

Correo electrónico

viv@viv.az

Servidor de correo

[102.130.118.158]

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre:	PDF-0027430505S3B101IF3.zip
SHA256:	5C4E6F90364DFEB19C1E7EA55B516F8BA211B2DCE1FF4F93B7C8DD32A61F2CC6
Nombre:	PDF-0027430505S3B101IF3.exe
SHA256:	85EB1D4FD5DC78552361BB1DA4422C0865BBAE3784470C2FAA551E461FB35D52

IoC URL

[https://5aa20a4eab0b.ngrok\[.\]io/PDF-0027430505S3B101IF3.zip](https://5aa20a4eab0b.ngrok[.]io/PDF-0027430505S3B101IF3.zip)

[https://makeupkala\[.\]com/well-known/acme-challenge/l/z/c218B3505l1016S502i3.zip](https://makeupkala[.]com/well-known/acme-challenge/l/z/c218B3505l1016S502i3.zip)

[https://zakatalquds\[.\]org/profiles/contts/hd218b0s5S20d1l322cj.php](https://zakatalquds[.]org/profiles/contts/hd218b0s5S20d1l322cj.php)

Imagen del mensaje

Estimado(A) Contribuyente

Servicio de Impuestos Internos (Sii) 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.



Le invitamos a regularizar esta situación a través de nuestro sitio web, en el menú **Recaudación / Pagos / Impuestos Fiscales**, a la brevedad posible, a fin evitar las molestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidas de apremio.

Puede descargar el informe generado por el SII en el siguiente enlace.

&n bsp;

[Descargar informe detallado](#)

Atención: Informe contraseña para ver su PDF. Nunca le des tu contraseña a nadie.
contraseña : 032022

Si ya realizó el pago, no considere el presente mensaje.
08/03/2022 03:28:28

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.