Alerta de seguridad informática	2CMV22-00349-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre 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 nueva campaña de phishing con malware. En ella, el mensaje es enviado desde una dirección de correo personal, y en él, el atacante habla de un supuesto proceso de emisión de una factura electrónica, adjuntándose un link hacia una página que imita al SII.

Si la victima hace clic en ese link, es redireccionada hacia otra página en donde se realiza la descarga de un archivo Zip con dos ejecutables en su interior. De ejecutar estos archivos, se realiza una recolección de información de las unidades de almacenamiento de la víctima, junto con un chequeo de las llaves de registro del sistema.

.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Asunto	Correo de Salida
☑ FACTURA - ERICA AMALIA , Notificacion Giro Folio 012210001 del 15/08/2022 - SII - - (984837087033)	dukcapiltapinkab@server.tapinkab.go.id

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre	SHA256
FACTURA-IDSE-34ed1ecf.zip	cc83ecc8da9069f2e3be95cee116d722163a3d104769711285f10543680849b3
FACTURA-IDSE-34ed1ecf-1a2c-4d26-85ba-bc0014sffe5001s4d.msi	9fbe66342de53d7ab1c7f3008bb8f5083c4400755903a27947e376da4661692a
hyr7wehds.exe	3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
dns-sd-documento-bajo_____ _____ _____.exe	6a27826b490457ccfecebaf98a01325cc1ccecc81917b156aa1e566d141b520c

Imagen del mensaje

[redacted], Este e-mail fue generado durante el proceso de emision de la factura electronica a la baja y remitida a usted conforme a la legislacion vigente.:

En el anexo sigue el archivo XML correspondiente a esta factura. Usted podra consultarla a traves del sitio Portal SII. Atencion: Informe contrasena para ver su PDF. Nunca le des tu contrasena a nadie. contrasena : 020105

— Ver la factura electronica :(1500Kb)

Atte: SII Chile Padre Alonso de Ovalle 698, Santiago, Region Metropolitana, Chile Email: contacto@sii.cl

22/08/2022 07:19:18

FALSO CSIRT

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: 2022.09.23 12:18:05 -03'00'