Alerta de seguridad informática	2CMV24-00440-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware suplantando al Servicio de Impuestos Internos con una falsa factura.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario dirigido principalmente a naciones de Iberoamérica.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
5a77ae65d77068dee0b029678b84f0234c4788a4de45e8f6f2390b1f09c7cee4	citacionpoderjudicl.zip
a510907486ad34776ddc8c47e08ebd98e985ff9c41b7aede9c8cdd011160a17d	citacionpoderjudicl.msi
36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068	l.txt
e28e34fbdaff077669586dcdb4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7	libeay32.dll
7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910a	ssleay32.dll
98c1f23e6e3176b902dd0446909a5065cbacbd4b3f15ea831d5b7ab01605bea6	ezexdqbe.dll

URL-Dominio

Dominio	Relación
https://ccpt.gov[.]ng/wps/01923i6C/0D17F5S33/01F3083.php?hash=66322708-ezintloslagos@interior.gov.cl	Descarga del Fichero
https://jw-ict[.]l/330215B8F11/776T0231CC/02722.php?/mail/0/inbox/id/AQMkADAwATNiZmYAZC1hNDU4LWRkADc2LTAwAi0wMAoARgAAA1kchXVlHz5CjfaazERwbi8HANHs14LD%2BI9Bt5SmE8UpN2gAAAIBDAAAA	Contenedor Malware
https://silviza[.]cl/mail/F981233/UC1023IF8B/home.php?hash=G-O-V	Contenedor Malware
Support-Sii@mail66322708[.]cl	Correo de salida
50.63.9[.]88	IP de correo de salida
18.221.32[.]222:9795	C2

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Consulta del Registro)	T1012
Descubrimiento (Información del Sistema)	T1082
Descubrimiento (Equipos Perimetrales)	T1120
Comando y control (Puerto no estándar)	T1571

Imagen del Mensaje

Fw: Informe Facturación Electrónica (Diciembre) - (7452803)

Depto.Facturacion <Support-Sii@mail66322708.cl>
Para [redacted]

Responder | Responder a todos | Reenviar

viernes 12-01-2024 5:18

[redacted]

Estimado contribuyente, su Facturación ya está disponible.

La información del Impuesto interno está disponible en formato PDF y Excel. Los hemos adjuntado al cuerpo de este correo. También puedes descargarla haciendo clic en el siguiente botón.

Tienes hasta el 15 de enero de 2024 para modificar tus datos de facturación de boletas de honorarios electrónicos. Después de esta fecha, no podrás hacer ningún cambio.

- Informe detallado-66322708.pdf(.pdf - Acrobat Reader)
- Informe detallado-66322708.excel(.excel - Microsoft Word)

Atentamente,

[redacted]

ATENCIÓN: Para una mejor visualización, abra en un ordenador (Windows).

FALSO CSIRT

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.12 16:59:58 -03'00'