Alerta de seguridad informática	2CMV24-00439-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 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 Poder judicial con una falsa citación.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario que destaca por el uso de comandos de base de datos SQL para obtener información del sistema infectado y así poder enviarlo a su servidor de Comando y Control.

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
192d51cd32647c1e7d5bc57560b4b6938caf5685bafa157edfc960d26a8e172a	bepiuzad.dll

URL-Dominio

Dominio	Relación
https://rao-romania[.]com/citacion/republicachilepoderjudicial/?hash={mail}	Descarga del Fichero
https://citrustalent[.]com/pk/citacionpoderjudicl.zip?999128620	Contenedor Malware
support@ontheballmedia[.]ie	Correo de salida
78.153.212[.]231	IP de correo de salida
139.144.212.80:8088	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 estandar)	T1571

Imagen del Mensaje

[SPAM]Citación de justicia para comparecimento ante el tribunal de justicia de Santiago.

PJ Poder Judicial - R e p u b l i c a d e C h i l e. <support@ontheballmedia.ie>
Para [redacted]

Responder | Responder a todos | Reenviar

martes 02-01-2024 22:42

Poder Judicial

Republica del Chile

FALSO CSIRT

Estimado Ciudadano

Atencion

Citacion para comparecimento ante el tribunal de justicia de Santiago, em Audiencia publica N2800122023/24 el dia 22/01/2024 Citación ***2820124/002***.
Para mas informacion vea el anexo online en el siguiente archivo abajo.

Información de citación: ***CitacionN*2820124/002.zip***

El archivo .zip solo estará disponible durante 7 días, si no lo visualiza se entenderá conforme a la acusación.

La falta de presentación de una defensa resultará en la detención automática.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.12 16:48:35 -03'00'