Alerta de seguridad informática	2CMV24-00447-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de febrero de 2023
Última revisión	28 de febrero 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 a la compañía general de electricidad con una falsa citación para un comparendo.
Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario dirigido principalmente a naciones de Iberoamérica (con distintas campañas que apuntan a distintos países, como la actual, preparada para Chile), y que destaca por el uso de comandos de base de datos SQL para obtener información del sistema infectado y enviarlo al servidor de Comando y Control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
c1e0f5185a2efc13b4e821ee1a2d445634e87fb380306315c482c05ae26fbd55	conasetnotificacioninfra.zip
17a6f57be6897d2a7456ad9b0f5bc798b951c6c41b2511886706edee16c5c14c	conasetnotificacioninfra.msi
\8ecc1fea5ca3169d8c6269ae0f1a13e3b1e7e9c415c6df4a77af08bd4a2dba11	bvcgvovg.dll
\913bbaede66f7c2f00b92916d5cad558067b589bca0b782409e96cb6bf48106e	lzmaextractor.dll

URL-Dominio

Dominio	Relación
https://alkebucentre.org/cgeboleta/facteletricidad/?hash={mail}	Descarga del Fichero
https://the-jazz-singer[.]co.uk/cgeboleta/nopagadanueva.zip?854560223	Contenedor Malware
support@twelvestepmiracle.com	Correo de salida
support@blog.pawstruck.com	Correo de salida
support@alwaysnbs.tv	Correo de salida
support@voresfriskole.dk	Correo de salida
67.227.226[.]138	IP de correo de salida
104.237.139[.]231:8088	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 estándar)	T1571

Imagen del Mensaje

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.28 17:37:30 -03'00'