Alerta de seguridad informática	2CMV24-00443-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de febrero de 2023
Última revisión	08 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 de transmisión y distribución eléctrica CGE.

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 enviarla a su 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
da93a526c95d0df08e9ab8d1fd6077d3f88c2f864e89aacb9aca8f963c7c776c	uqaqmgf.dll
52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e	aicustact.dll
0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	SoftwareDetector.dll

URL-Dominio

Dominio	Relación
https://garbasrealestate[.]com/cge/facteletricidad/?hash={mail}	Descarga del Fichero
https://conveyancingteam[.]co.za/mymuword/factcgeeletricdad.zip?447307028	Contenedor Malware
support@de.trexel.com	Correo de salida
support@masterelia.com	Correo de salida
support@tfilter.dreams.sa	Correo de salida
support@ambaniorganics.com	Correo de salida
support@alwaysnbs.tv	Correo de salida
support@osangjaiel.co.kr	Correo de salida
104.207.254[.]61	IP de correo de salida
172.105.41.109:8088	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: 2024.02.08 17:16:11 -03'00'