Alerta de seguridad informática	2CMV23-00423-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de julio de 2023
Última revisión	12 de julio 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 que se difunde a través de emails que suplantan al Ministerio de Transportes y Telecomunicaciones, aduciendo una supuesta multa (que en realidad es inexistente)

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario que apunta principalmente a Brasil, Chile, México, España, Perú y Portugal, y cuya característica más destacada en las variantes más recientes es el uso de una base de datos SQL como servidor de C2.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
bc5b31facbded74c5fd435198a28ffad8e9191bcb7af3fccd6671de3849e08af	MTT0001221000MULT4411s4a000.zip
be77fceb122776f894dea1a78d076cf4e667044a9fcadf781a613a4bc93d16ee	MTT0001221000MULT4411s4a000.msi

URL-Dominio

Dominio	Relación
https://p-tekng.com/wp-content/themes/--/NEX/dasssashytsrfwewdw4w432dcadssswe32dsfwywyw67wjjehnsbvcdfreyd.php	Descarga del Fichero

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

Imagen del Mensaje

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.12 14:45:49 -04'00'