Alerta de seguridad informática	2CMV23-00421-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de junio de 2023
Última revisión	28 de junio 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 suplanta a Chilexpress, difundida en emails que falsamente avisan de una supuesta encomienda recibida.

Si la víctima interactúa con el fichero malicioso se encuentra con Mekotio, un troyano bancario cuya característica más notable 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
1fc3c3ad207309eede611ccafe91035b75163fd1fcf37db6fc61a6b251bcfe78	FormularioimprimibleCLexpress.zip
c3dd7c57ce52dd98cdac96e7bbb3c9b99fe55f1b62989f793ad8eb68d29c1e70	FormularioimprimibleCLexpress.msi
d8c9ea8a886e7e97048aaddb113f3220ed47535942cc3951316cab1a9489605e	clexpressFormularioimprimible.zip
07341bf5f2e5b9bf5cc9179a9a93b6eaee4417f92498d348933ea09e0742e055	clexpressFormularioimprimible.msi

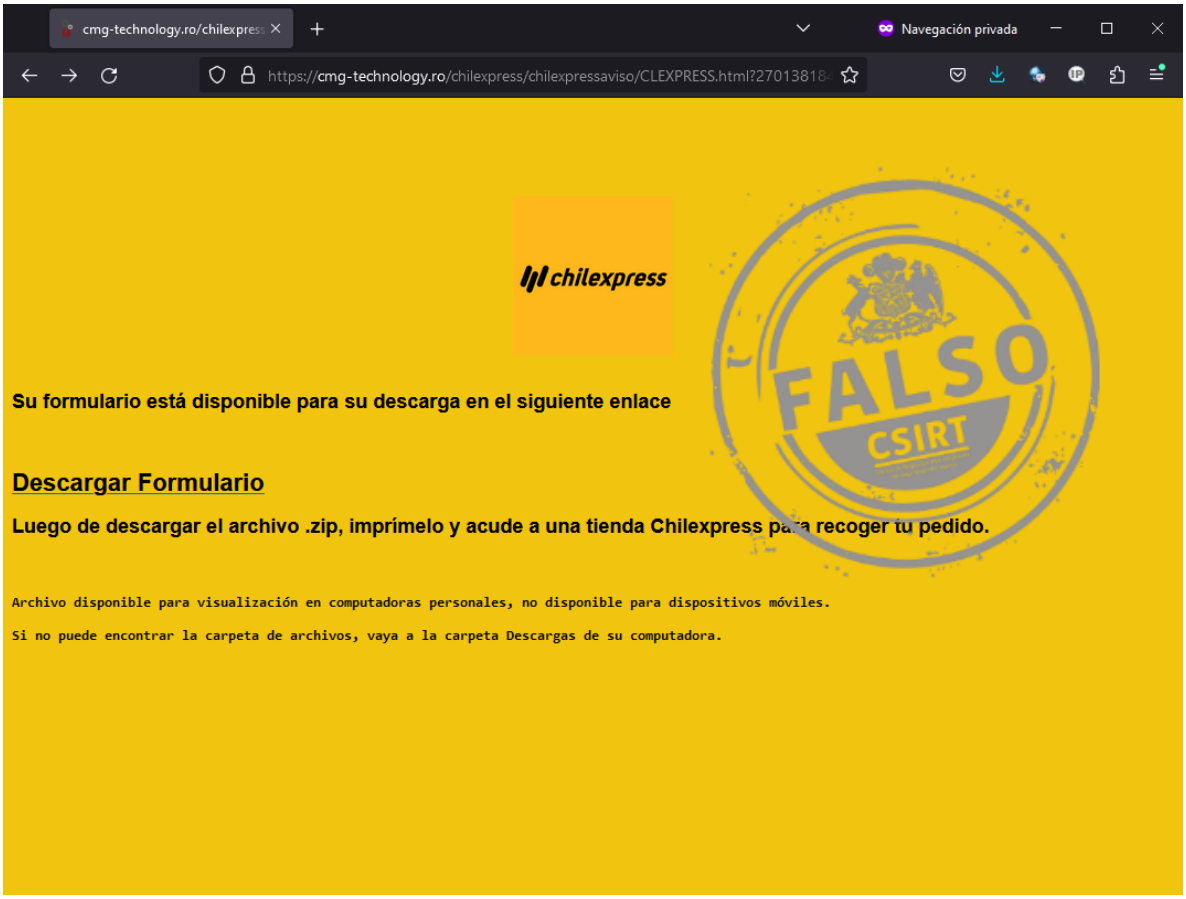
URL-Dominio

Dominio	Relación
https://cmg-technology[.]ro/chilexpress/chilexpressaviso/CLEXPRESS.html?270138184	Descarga del Fichero
https://nabaacademy[.]com/vendor/chilexpress/	Contenedor de Malware

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: 2023.06.28 12:26:40 -04'00'