Alerta de seguridad informática	2CMV23-00430-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2023
Última revisión	13 de octubre 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 estudio de abogados mexicano ProLegal con una falsa cotización.

Si la víctima interactúa con el fichero malicioso se encontrará con una explotación de vulnerabilidad en Microsoft Office que permite a los atacantes ejecutar código remoto en el sistema. Esta vulnerabilidad esta relacionada con el antiguo editor de ecuaciones de Office (EQNEDT32.EXE), el cual no maneja correctamente los objetos en memoria. Esta herramienta permite a los usuarios insertar ecuaciones matemáticas como objetos OLE dinámicos en documentos de Office.

Este archivo Excel también transporta un malware llamado Agent tesla. Este malware es una amenaza del tipo troyano de acceso remoto (RAT) que esta destinado a sustraer información de sus víctimas. Dentro de estas capacidades registra lo que se digita (keylogger), toma capturas de pantalla, visualiza y copia lo que hay en el portapapeles, extrae contraseñas y cookies de múltiples navegadores web, VPN (Open VPN, Nord VPN) y también de Microsoft Outlook.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
e418ac2813daadef8ed238148ab1b1037567e126271316157d7955b2ce6fa858	solicitud de cotización.xlam
1e3e163f9796bf7a5bfd120a3fa29cd1ca5487f740e2b669bfb766d74096bcd3	blalalalalalalala.hta
5afa7469bccc0b7357d39e8a75cba0a52d44b85de2d9c5a78a0e0c12cef03c06	hta_nostartup.jpg
b67634b988dfb1f43e7ecd30579fe285e1e57740d646f6896b4f6a0d13cfb9dd	zQVpAqjgf.exe
584e458ff9e83bced5806448aa5a1b678002e9c7cc92a48901c2bb48f9bad29b	Fiber.dll

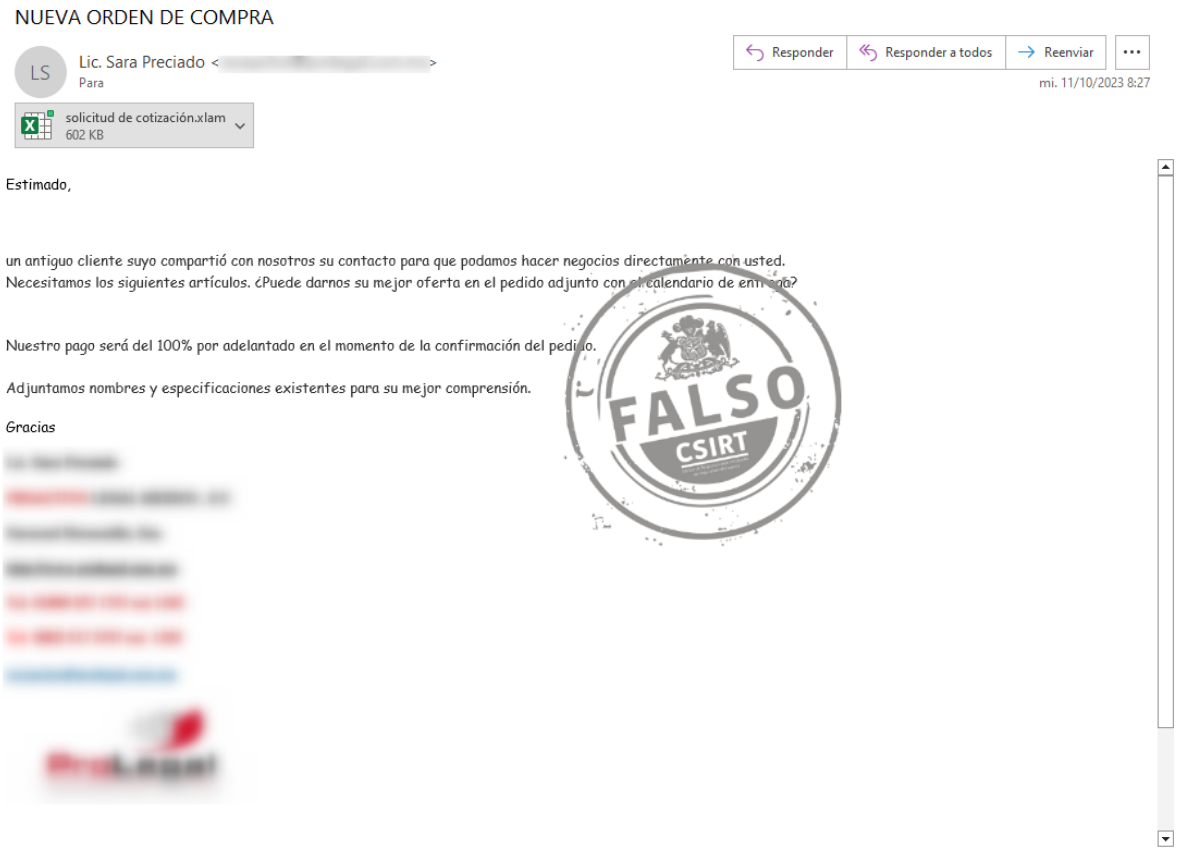
URL-Dominio

Dominio	Relación
https://uploaddeimagens[.]com.br/images/004/583/414/original/hta_nostartup.jpg?1692658645	Descarga del Fichero
http://185.225.74[.]170/realonerealone.txt	Configuración Malware

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Consulta del Registro)	T1012
Descubrimiento (Información del Sistema)	T1082
Ejecución (Explotación para ejecución en cliente)	T1203
Acceso a credenciales (credenciales en archivos)	T1081
Colección (Datos del sistema local)	T1005
Colección (Colección Email)	T1114

Imagen del Mensaje



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.13 14:56:32 -03'00'