Alerta de seguridad informática	2CMV23-00426-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2023
Última revisión	18 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 una falsa cotización.

Si la víctima interactúa con el fichero malicioso se encontrará con un archivo de Microsoft Excel que explota una vulnerabilidad de Office que permite a los atacantes ejecutar código remoto en el sistema. La vulnerabilidad está relacionada con el antiguo editor de ecuaciones de Microsoft 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.

El archivo Excel maliciosa transporta un malware llamado Agent Tesla, un troyano de acceso remoto (RAT) diseñado para sustraer información de sus víctimas. Para eso, registra lo que se digita en el equipo infectado (función keylogger), toma capturas de pantalla, visualiza y copia lo que hay en el portapapeles, y extrae contraseñas y cookies de múltiples navegadores web, VPN (como Open VPN y Nord VPN) y también de Microsoft Outlook.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
6cf5eb81d932e600c8ca6662cdd81fad871d2a31733a39154862062782d1a58b	096554365cotización.xlsx
650ae74cf998803602f93dbcc56b25ccb13b4d45914be507511cbf5fe619007f	docthursday.vbs
7c451d9ecb10e2a1aa4512e56ab3859675ab3f28aa40d3c63e45e4e8c35b10cb	PPZrQQAxIGIYpWRhmWDcUPp.vbs
0ace5259a5f3de5bfd71221aac959b8054bc31018aac425aa440aa4fe451ebb8	agent_tesla.exe

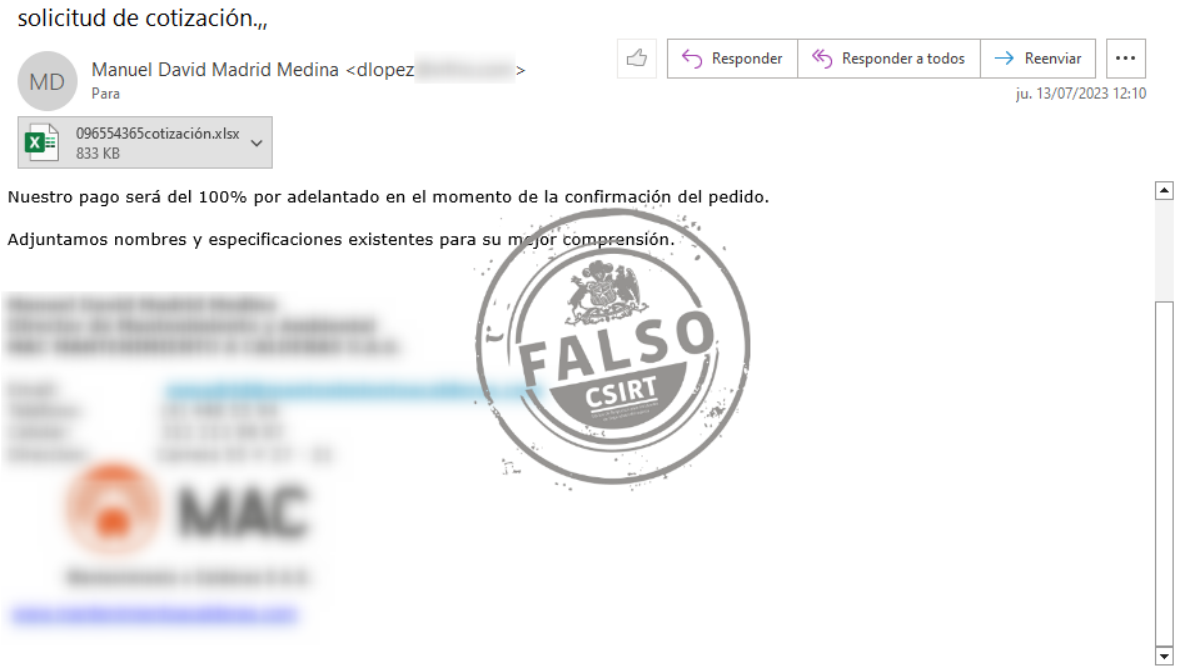
URL-Dominio

Dominio	Relación
http://195.178.120[.]24/PPZrQQAxIGIYpWRhmWDcUPp.vbs	Descarga del Fichero
http://servidorarquivos.duckdns[.]org/e/e	Comando y control

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: 2023.07.18 17:09:37 -04'00'