Alerta de seguridad informática	2CMV23-00431-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de noviembre de 2023
Última revisión	03 de noviembre 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 la empresa Pevisa con una falsa solicitud de compra.

En su lugar, el documento adjunto incluye al malware conocido como Agent Tesla, el que sustrae información confidencial y la envía a los atacantes. Para realizarlo, busca las credenciales de usuario que se almacenan en diferentes programas como navegadores, clientes de correo electrónico, clientes FTP/SCP, bases de datos, herramientas de administración remota, aplicaciones VPN y de mensajería instantánea. Más aún, este malware es capaz de robar datos que se encuentren en el portapapeles, grabar las pulsaciones del teclado (función de keylogger) y hacer capturas de pantalla.

Finalmente, Agent Tesla envía la información sustraída por medio de correo electrónico, Telegram, o subiéndolos a algún sitio web o servidor de FTP.

Indicadores de compromiso asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
510771c843a856eb15d763d0931002f6f297aed35b0ed9aac509d3bd6e7b964a	Factura de proforma___xlxs.7z
b0b873b46d9e024e7d59de49d506637f2bb31632465ccf88424ca1ab3c457b38	Factura de proforma___xlxs.exe

URL-Dominio

Dominio	Relación
https://telemas[.]com.co/cdi/Djphbrnppqe.pdf	Validación
https://api.telegram[.]org/bot6548288330:AAGA-b1ojgiCCinc5YQor8R1kxgez4hPFpM/sendDocument	Comando y control

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Acceso a credenciales (Credenciales no aseguradas)	T1552
Acceso a credenciales (Credenciales en Archivos)	T1552.001
Colección (Datos del sistema local)	T1005

Imagen del mensaje

FACTURA DE PROFORMA

J Jorge <
Para

Responder | Responder a todos | Reenviar | ...

mi. 01/11/2023 19:32

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Factura de proforma__xlxs.7z
45 KB

Estimado señor,

Buenos dias

Perdón por el retraso, adjunto lo siguiente para su referencia.

- Certificado de origen
- Factura de proforma
- Lista de embalaje

Documentos autorizados por usted. Gracias de antemano por su amable cooperación.

¡Gracias y Saludos cordiales!