Alerta de seguridad informática	2CMV23-00434-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de noviembre de 2023
Última revisión	08 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, el que se propaga en un archivo adjunto que simula ser una falsa postulación a un puesto laboral.

El malware que distribuye esta campaña es Agent Tesla, programa malicioso que sustrae información confidencial y la envía a los atacantes. Para eso, roba datos almacenados en programas como navegadores, clientes de correo electrónico, clientes FTP/SCP, bases de datos, herramientas de administración remota, aplicaciones VPN y de mensajería instantánea. Además, este malware es capaz de robar datos que se encuentren en el portapapeles, grabar las pulsaciones del teclado y realizar capturas de pantalla.

Agent Tesla envía toda la información sustraída a los atacantes por medio de correo electrónico, Telegram, Discord o subiéndolos a un sitio web o un servidor de FTP.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
0e9ee8e1f09d84f6d77878591c6f15a818b38e636022becab44f5630d5cf6af5	2023-11 CV Forner Eugenia.zip
df3035bf5b05466757706b2b5ef5028b7ada1227ae0d1b73314c71a6026f1239	2023-11 CV Forner Eugenia.exe

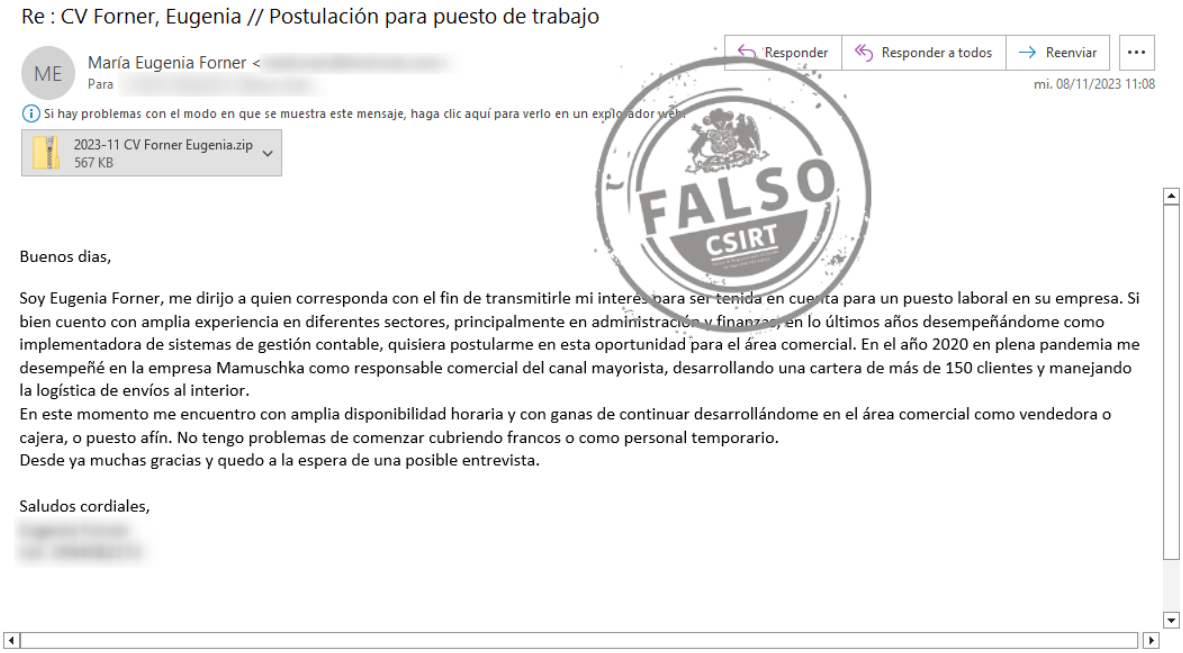
URL-Dominio

Dominio	Relación
https://discord[.]com/api/webhooks/1171723200741257216/Gcyp-_pKpHXDEZGtrdsBTGVDcc2OYUckNC6AxqbtT3aDfY8F2m1FbeqnjbOgcclH0Zqy	Comando y control

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.001
Ejecución (Explotación para la ejecución de clientes)	T1203
Acceso a credenciales (Credenciales no aseguradas)	T1552
Acceso a credenciales (Credenciales en Archivos)	T1552.001
Colección (Datos del sistema local)	T1005
Comando y control (Servicio Web)	T1102

Imagen del Mensaje



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.08 17:48:41 -03'00'