Alerta de seguridad informática	2CMV23-00428-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de agosto de 2023
Última revisión	29 de agosto de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior ha identificado una nueva campaña de phishing con malware que suplanta a una persona natural con un falso currículum vitae, como si estuviera respondiendo a un aviso laboral. El documento adjunto al email es realmente un archivo malicioso.

Si la víctima interactúa con el fichero malicioso se encontrará con Agent Tesla, un malware de tipo troyano de acceso remoto (RAT). Una vez desplegado, Agent Tesla realiza registros de lo que se ingresa en el teclado (keylogger), toma capturas de pantalla, copia el contenido del portapapeles, sustrae contraseñas de programas como navegadores web y Outlook, además de recopilar información del equipo infectado. Toda esta información la envía luego a los ciberdelincuentes y con su comando y control a través del protocolo SMTP (puerto 25) o incluso por Telegram o Discord.

Otra de las características importantes de Agent Tesla es su capacidad de establecer su persistencia, inciándose cada vez que se reinicie el equipo.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
819b818549255b76077e9033d8450b6731d43998df92e5f45a7cda660c0bce0e	CV AUG 2023.zip
edc17b778240c4aa6910af9803166fc092513782e101df115048c545683dce66	CV AUG 2023.exe

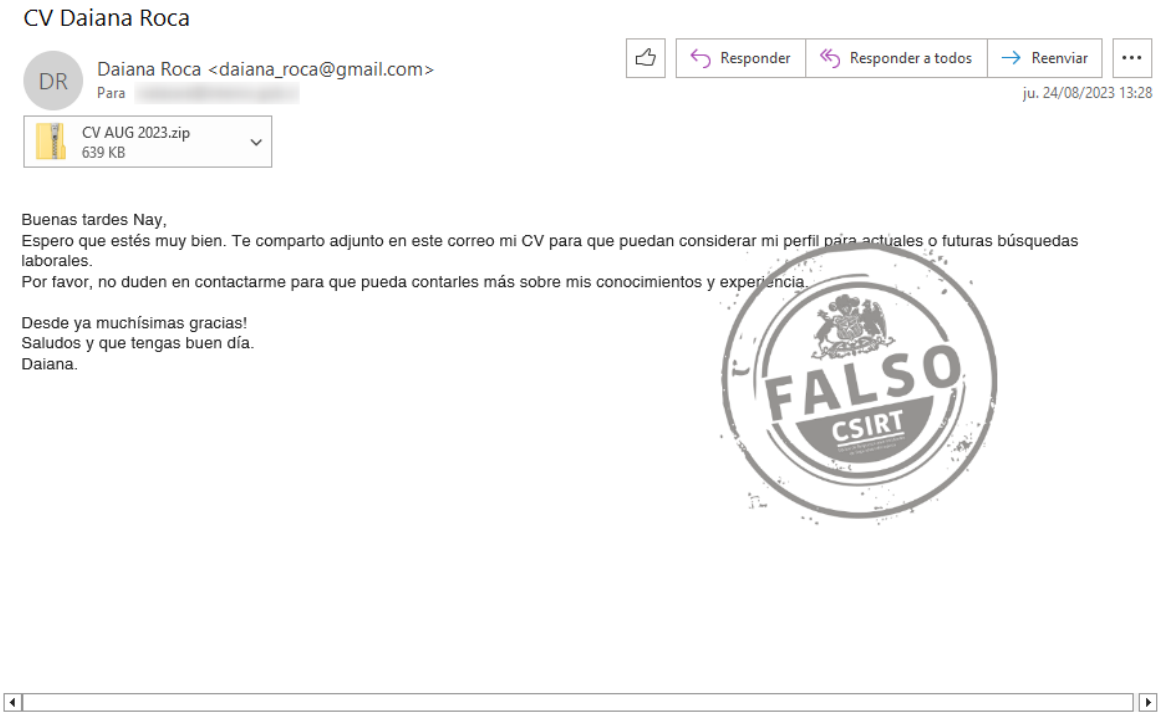
URL-Dominio

Dominio	Relación
https://discordapp.com/api/webhooks/1137023390029459558/ldz8S9vhgT9q0YyJluiWCS8K8CG_TiDgPSszw3j3WD-7RiiwgdrOqropK3lNmkTJqLC6	Comando y Control

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Credenciales de Acceso (Credenciales no seguras)	T1552
Credenciales de Acceso (Credenciales en Archivos)	T1552.001
Colección (Información del sistema local)	T1005

Imagen del mensaje



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.06 17:31:35 -03'00'