Alerta de seguridad informática	2CMV23-00433-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de noviembre de 2023
Última revisión	06 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 Universidad de Chile con un email que exige respuesta urgente a unos supuestos requisitos pendientes para la producción de supuestos artículos.

En realidad, los adjuntos corresponden a archivos de malware. En este caso, se trata de dos malware funcionando en conjunto: Guloader y Lokibot.

Guloader es un malware que suele ser distribuido por medio de correos electrónicos de phishing, con el objetivo de descargar y ejecutar otros malware del tipo stealer o RAT. Lokibot es un malware diseñado para el robo de información y credenciales desde navegadores web, como cuentas bancarias y correos electrónicos, entre otras aplicaciones. Además, es keylogger y permite recibir información de comando y control.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
8e52dd0278b75ba5b0411951d8397e5ce7813dfff9ccffcb3e2d21eab71604a1	Solicitud de Cotización Urgente (202310_30432UCH-CL)·pdf.rar
c8f3bc71f3d8339af58bdfc7054bbb8436a1a52b41d86ac33c735f627bcbace3	Solicitud de Cotización Urgente (202310_30432UCH-CL)·pdf.vbs

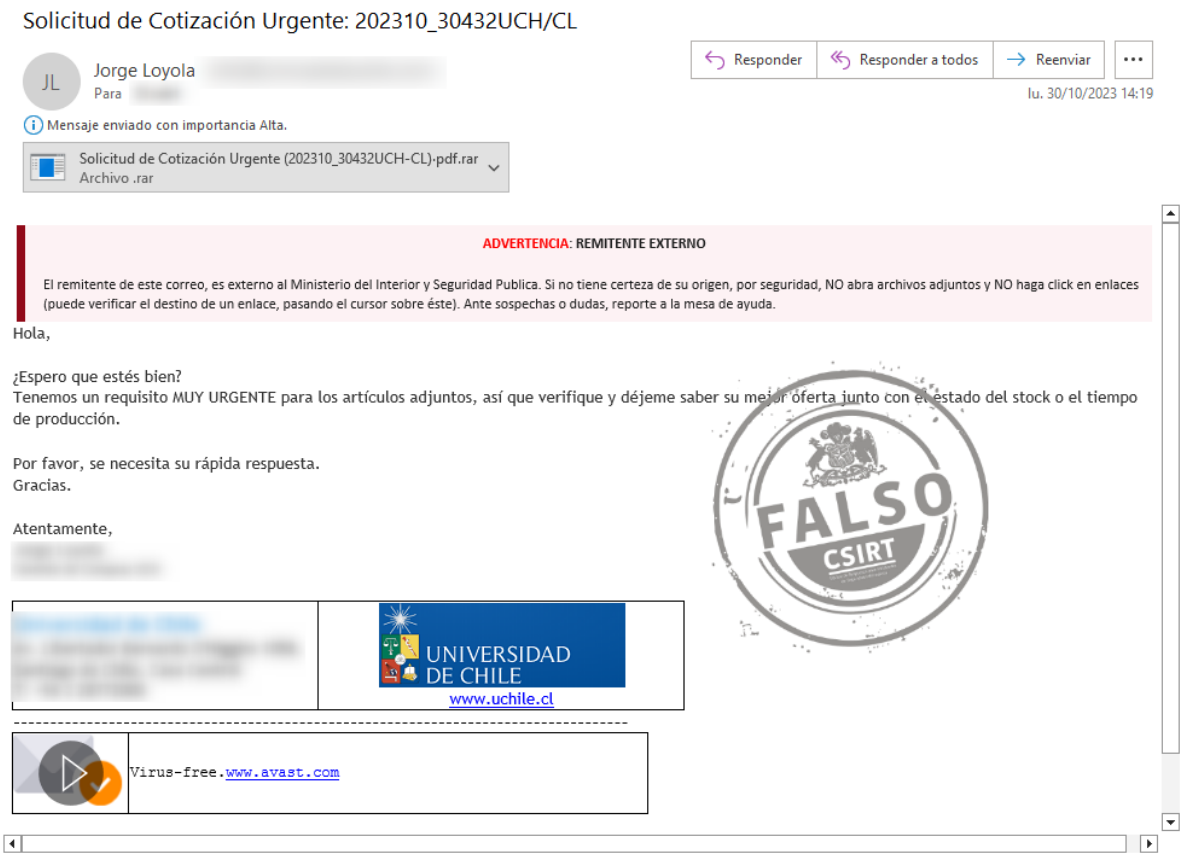
URL-Dominio

Dominio	Relación
https://drive.google[.]com/uc?export=download&id=1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
https://doc-00-c4-docs.googleusercontent[.]com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/thoc2tionc5fg4pm29mmucd39cal2chm/1699284900000/15460567426367328879/*/1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7?e=download&uuid=d16c2812-aea1-4b95-bd02-485c17e0d88a	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
https://drive.google[.]com/uc?export=download&id=1R2oKSmimiwjQppJp7FLYWk5PfZXuKfGc	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
http://146.190.157[.]174/NcBb73GzfMtT6Sl	Lokibot

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.001
Ejecución (Explotación para la ejecución de clientes)	T1203
Descubrimiento (Descubrimiento de información del sistema)	T1082
Colección (Colección de correos)	T1114
Comando y control (Servicio Web)	T1102

Imagen del Mensaje



CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.07 14:54:37 -03'00'