

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior



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.

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
8e52dd0278b75ba5b0411951d8397e5ce7813dfff9ccffcb3e2d21eab71604a1	Solicitud de Cotización Urgente (202310_30432UCH-CL).pdf.rar
c8f3bc71f3d8339af58bdfc7054bbb8436a1a52b41d86ac33c735f627bcbase3	Solicitud de Cotización Urgente (202310_30432UCH-CL).pdf.vbs

URL-Dominio

Dominio	Relación
https://drive.google[.]com/uc?export=download&id=1R4xBOHz985Aknw3uj5Q6NpAXJ3vb aqp7	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
https://doc-00-c4-docs.googleusercontent[.]com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/thoc2 tionc5fg4pm29mmucd39cal2chm/1699284900000/15460567426367328879*/1R4xBOHz 985Aknw3uj5Q6NpAXJ3vbaqp7?e=download&uuiid=d16c2812-aea1-4b95-bd02- 485c17e0d88a	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
https://drive.google[.]com/uc?export=download&id=1R2oKSmimiwjQppJp7FLYWk5PfZXuK fGc	Abuso de servicios de alojamiento legítimos para alojar programas maliciosos/C2
http://146.190.157[.]174/NcBb73GzfMtT6SI	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

CONTACTO Y REDES SOCIALES CSIRT

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior

Imagen del Mensaje

Solicitud de Cotización Urgente: 202310_30432UCH/CL



Jorge Loyola
Para [Redacted]

Responder Responder a todos Reenviar

lu. 30/10/2023 14:19

Mensaje enviado con importancia Alta.

Solicitud de Cotización Urgente (202310_30432UCH-CL)-pdf.rar
Archivo .rar

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Pública. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.

Hola,

¿Espero que estés bien?

Tenemos un requisito MUY URGENTE para los artículos adjuntos, así que verifique y déjeme saber su mejor oferta junto con el estado del stock o el tiempo de producción.

Por favor, se necesita su rápida respuesta.
Gracias.

Atentamente,

[Redacted Signature]



CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>