

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	2CMV23-00432-01
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 suplantando a la empresa Ditter con una falsa nota de crédito.

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.

CONTACTO Y REDES SOCIALES CSIRT

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

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
6a457eb922af750f662dbbdcc59386c742538066c222a298c04175d4a5e802fd	Nota de credito.zip
4d7b65d0e759355d6b6295db58ad985efdd04f01e80e1c34bfc8c39787735a44	Nota de credito.exe
b0941553bf71a3d7dbc296f544d5b00832e6207cfdaaa6cdec2bf6a8a3dc39a8	PR2310-11198.zip
4d7b65d0e759355d6b6295db58ad985efdd04f01e80e1c34bfc8c39787735a44	PR2310-11198.exe

URL-Dominio

Dominio	Relación
https://discord[.]com/api/webhooks/1169917901906653224/YjkyFWX_CawSIPQ02zeV3XExHGtDteoh-fLuvdqIFqL772Pb__cJUtnVv4DqDRhm0ks1	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

CONTACTO Y REDES SOCIALES CSIRT

Imagen del Mensaje

Re : Solicitud de Aprobación Nota de Crédito

DN D [Redacted] <[Redacted]>
Para [Redacted]

Nota de credito.zip 570 KB
PR2310-11198.zip 570 KB

Responder Responder a todos Reenviar ...
vi. 03/11/2023 20:17

Buen día,

Junto con saludarles, adjunto solicitud para realizar una nota de crédito, esto es para el cliente de Danisco el cual hizo devolución del producto. Esta factura corresponde al mes de septiembre la cual no será refacturada ya que el cliente se le entregó otra alternativa más costosa, que se encuentra pendiente de ser aceptada (adjunto cotización).

El documento se encuentra en el plazo para ser anulado hasta noviembre en donde se cumple el plazo de los tres meses, para generar la nota sin perder impuesto.

Quedo atenta a sus comentarios,

Saludos Cordiales,



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>